|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification details** | | | |
| **Training Package Code and Title:** | **ICT - Information and Communications Technology (Release 8)** | | |
| **Qualification National Code and Title:** | ICT50220 - Diploma of Information Technology (Release 2.0) | **State code:** | BGJ4 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Assessment Title** | **AT2 Project** | | |
| **Unit National Code & Title** | BSBXCS402 - Promote workplace cyber security awareness and best practices (Release 1) | | |
| **Date Due** | **Week 18** | **Date Received** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Student Name** |  | **Student ID** |  |
| **Student Declaration** | I declare that the evidence submitted is my own work:  ………………………………………….. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Assessor Name** |  | | | |
| **Assessment Decision** | Satisfactory | | Not Yet Satisfactory | |
| **Assessor Signature** |  | | **Date** |  |
| **Is student eligible for reassessment (Re-sit)?** | No | Yes | **Reassessment Date:** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Feedback to student** | | | |
| *Via Blackboard (LMS) – Please check [Grade] section.* | | | |
| **Feedback from student** | | | |
| *Via Blackboard (LMS) – Please use [Comment] section during submission.* | | | |
| **Student signature** |  | **Date** |  |

|  |
| --- |
| **Assessment Instructions** |

|  |  |
| --- | --- |
| **TO THE ASSESSOR** | |
| Type of Assessment | Project |
| Duration of Assessment | 8 Class Sessions (Week 11 - 18) |
| Location of Assessment | Classroom, Designated Lab, Home |
| Conditions | Learners are required to complete the required tasks in class and at home, where suitable, and submit the required documentation electronically via Blackboard |
| Elements and Criteria | As detailed in the assessment plan |

|  |  |
| --- | --- |
| **TO THE STUDENT** | |
| Purpose of Assessment | You are required to show you can:   * Develop cyber security awareness in work area * Support effective cyber security practices in work area * Review cyber security awareness in work area |
| Allowable Materials | Blackboard (Topic by topic) will include the following: Weekly Readings, Class notes, and Weekly Activities. |
| Required Resources | Computer with:   * Internet Access * Word processing software * Access to Learning Management System (LMS) * Access to Allowable Materials * Access to Office 365 |
| Reasonable Adjustment | In some circumstances, adjustments to assessments may be made for you. If you require support for literacy and numeracy issues; support for hearing, sight or mobility issues; change to assessment times/venues; use of special or adaptive technology; considerations relating to age, gender and cultural beliefs; format of assessment materials; or presence of a scribe you need to inform your lecturer. |
| Assessment Submission | All questions and activities must be attempted.  Use of research tools and peers in formulating answers are acceptable – but work submitted must be your own work.  Final project documentation is to be uploaded to the appropriate area in the Blackboard course created for this unit.  If you are marked as NYS (Not Yet Satisfactory) on your first attempt, you will be provided with another opportunity to re-attempt the assessment, within the DAP timeframes and as per SMTAFE policy. Any further submissions will be at the discretion of the lecturer. |
| Project contents | This project consists of the following tasks:   * Establish current level of awareness in work area relating to cyber security * Create and maintain cyber security awareness program that reflects organisation-wide best practice * Contribute to developing cyber security policies and procedures, and communicate to required personnel * Review cyber security practices according to organisational policies and procedures * Arrange training and information updates as required, and maintain related records * Present insights from review and training to required personnel, and potential related impacts on workplace * Review latest cyber security threats and trends impacting organisations * Document outcomes of review and suggested improvements for consideration by required personnel * Communicate review outcomes and cyber security improvement requirements according to organisational policies and procedures |

Your assessor will use the following checklist to assess your understanding of the issues and participation and communications skills for this competency.

| **Did the candidate demonstrate the ability to do the following:** | **Yes** | **No** | **Assessor Comments:**  *(This section must contain lecturer’s notes/comments)* |
| --- | --- | --- | --- |
| **Activity 1: Development** |  |  |  |
| * Establish current level of awareness in work area relating to cyber security |  |  |  |
| * Create and maintain cyber security awareness program that reflects organisation-wide best practice |  |  |  |
| * Contribute to developing cyber security policies and procedures, and communicate to required personnel |  |  |  |
| **Activity 2: Training** |  |  |  |
| * Review cyber security practices according to organisational policies and procedures |  |  |  |
| * Arrange training and information updates as required, and maintain related records |  |  |  |
| * Present insights from review and training to required personnel, and potential related impacts on workplace |  |  |  |
| **Activity 3: Review and Reporting** |  |  |  |
| * Review latest cyber security threats and trends impacting organisations |  |  |  |
| * Document outcomes of review and suggested improvements for consideration by required personnel |  |  |  |
| * Communicate review outcomes and cyber security improvement requirements according to organisational policies and procedures |  |  |  |

*Continue to the next page*

**ASSESSMENT SUBMISSION CHECKLIST**

Use the checklist below to ensure you have submitted all the necessary files

|  |  |
| --- | --- |
| **Activity 1** | **Check** |
| Updated Password Policy |  |
| Created Clean Desk Policy |  |
| PowerPoint slides for Password Policy |  |
| PowerPoint slides for Clean Desk Policy |  |

|  |  |
| --- | --- |
| **Activity 2** | **Check** |
| Signed off Activity 2 meeting signoff sheet |  |
| 2x Screenshots of sent emails with calendar invites |  |
| 2x Screenshots of demonstrating sharing PowerPoints |  |
| One page proposed training summary |  |

|  |  |
| --- | --- |
| **Activity 3** | **Check** |
| 2x Final drafted and proof-read reports |  |
| Communication screenshots attached to end of the report document |  |

|  |
| --- |
| **Scenarios** |
| *You are a member of the CITE MS Information Security team, you work directly under and report to the CITE MS Chief Security Officer (CSO). You have been tasked with analysing current policies and processes to see where there are gaps that need to be addressed. Two immediate issues were noticed, regarding the existing password policy and a lack of a clean desk policy. You are also required to create training materials and organise training sessions, as well as perform reviews of standards, organisational processes, and make recommendations.*  Scenario 1 - Existing bad password policy:  *CITE MS is using a password policy that was designed by one of the previous Information Security Managers, however this was created nearly 10 years ago. While old, staff found it easy to use and follow and as such it has not been updated since its creation. However, due to the age of the policy a number of the parts are well and truly out of date. It is your task to update the policy to be in line with modern day best practices.*  Scenario 2 - Creating a clean desk policy:  *Management at CITE MS have requested that a clean desk policy is to be created due to the previous attack where a support team staff member’s credentials were compromised due leaving out written-down usernames and passwords on their desk. You are to create the policy which will dictate how staff need to manage their desks, their workstations, and any physically recorded information or storage media that needs to be stored.* |

|  |
| --- |
| **Activity 1: Development** |
| 1. Read over the above scenarios and the provided policy documents. 2. Update the current password policy so that it aligns with modern best practices for organisations. To do this use the policy template provided. Ensure that all sections are filled out and it has met all the requirements of the provided scenario and documentation. 3. Create a Clean Desk Policy. To do this use the policy template provided. Ensure that all sections are filled out and it has met all the requirements of the provided scenario and documentation. 4. You now need to plan out how you will develop the security awareness program to go with the policy and process changes created by the previous steps. The target audience for this training are the support staff, who may have technical knowledge but not deep security knowledge. Create a set of PowerPoint presentation slides (one for Activity 1.2 and another for Activity 1.3) which includes:    1. An introduction to the topic    2. A summary of the policy that includes a paragraph about why it is important in the workplace and what can occur if staff don’t follow it    3. The points of the policy you have created |

|  |
| --- |
| **Activity 2: Training** |
| 1. Once you have finished Activity 1, meet with your supervisor (your lecturer) to obtain signoff of your training materials and plan for your training sessions. To prepare for this, review and write up a brief set of notes on what the current policies and procedures are, why they are lacking, and what you propose in the new policies to address the noted problems. 2. Invite one of the support staff (a classmate) to **two separate** security awareness policy training sessions for what has been created in activity 1.2 and 1.3 via Outlook365 calendar invites and send them the information about the meeting. These emails should include:    * an appropriate subject line    * a greeting    * a brief explanation into what the training is about    * the importance of the training (from activity 1.4)    * location, date, and time    * attached training materials    * signature   Further, share the training materials with the staff member using OneDrive’s file sharing settings.  Take a screenshot of the calendar invite email and the OneDrive file sharing invite to demonstrate this.   1. Write a one page proposed training summary that includes the following:  * What was proposed for the training. * The outcome of your review of the current policies and procedures. * What was changed in response to your review and why. * What goals do the training sessions have for the work area? |

|  |
| --- |
| **Activity 3: Review and Reporting** |
| 1. Management have advised that after seeing the recommendations for improvements, they want to ensure that they are doing all they can to be in line with modern accepted standards and to protect against the latest cyber security threats and trends impacting organisations. As such, they want to focus on the threat vectors of passwords and contracted staff. They have curated a number of information sources they want you to analyse.   Review the following sources:   * + 1. Passwords: <https://pages.nist.gov/800-63-3/sp800-63b.html> (Focus on section 5.1.1 and Appendix A)     2. Insider attacks using contractors: <https://techmonitor.ai/technology/hardware/cyber-criminals-cleaners>  1. Write **two** reports (approximately one page each) of further suggested changes to policy/process based on the previous step for both topics. The target audience for these reports is your immediate supervisor. This review should include:    * Introduction (introduce the topic and what are the topics you will discuss)    * Recent changes to policies (as part of activity 1 and 2)    * Summary of the report (reviewed in activity 3.1)    * Link what steps or actions currently are **and** what are not in line with the report    * Conclusion (discuss the major findings throughout this process)    * Recommendations (what changes should be implemented from here) 2. After you have finished and proof read your reports, send two emails to your immediate supervisor (lecturer) to discuss each of the reviews/reports. Ensure that the emails include:    * an appropriate subject line    * a greeting    * a brief explanation of the review and your findings    * your recommendations    * attached report (from activity 3.2)    * signature   Take a screenshot of the email and insert it at the end of the associated report. |