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

|  |  |  |  |
| --- | --- | --- | --- |
| **Assessment Title** | **AT1 Knowledge Evidence (KE)** | | |
| **Unit National Code & Title** | BSBXCS402 - Promote workplace cyber security awareness and best practices (Release 1) | | |
| **Date Due** | **Week 10** | **Date Received** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Student Name** | **Samuel Bailey** | **Student ID** | 30106121 |
| **Student Declaration** | I declare that the evidence submitted is my own work:  …SBailey……….. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 | Written |
| Duration of Assessment | 2 Class Sessions (Week 9 - 10) |
| Location of Assessment | Classroom, Designated Lab, Home |
| Conditions | Learners are required to complete the questions in class and at home, 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 demonstrate understand of:   * legislative requirements relating to cyber security context of performance evidence, including: * data protection * implications of Notifiable Data Breach legislation on an organisation and other associated Australian privacy laws * established international legislation * organisational policies and procedures relating to: * securely storing, sharing and managing information * encryption, and protocols for its uses * data classification and management * media/document labelling * data governance * acceptable use * bring your own device * Australian government sources of information on current threats * risks associated with workplace cyber security * strategies and techniques for promoting workplace cyber security * techniques for: * implementing and promoting workplace cyber security awareness * facilitating training that promotes cyber security awareness, including the use of simulated activities. |

|  |  |
| --- | --- |
| Allowable Materials | Blackboard (Topic by topic) will include the following: Weekly Readings, Class notes, and Weekly Activities. |
| Required Resources | Computer with:   * Internet Access * Access to Office 365 * Word processing software * Access to Learning Management System (LMS) * Access to Allowable Materials |
| 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 must be attempted.  Use of research tools and peers in formulating answers are acceptable – but work submitted must be your own work.  Final document 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 at the discretion of the lecturer. |

|  |
| --- |
| **Scenario** |
| **Scenario**: *You are a security administrator for CITE MS, which has had a recent successful attack whereby a staff member’s credentials were stolen from a ‘black book’ on their work desk and then used to exfiltrate customer personally identifiable information and payment information. Management have tasked you with re-evaluating the current policies related to security, ensuring that they are in-line with legislation, and to provide training for existing staff to improve their cyber hygiene.*  *The following questions have been proposed to you by management in order to gauge your understanding and to start the process of checking and/or creating policies, where some may be missing, as well as planning user education, training, and awareness.*  Fully answer all questions in detail and submit to the lecturer via Blackboard as an electronic copy. Any and all external sources used to inform your answers (images, websites, articles, or otherwise) need to be referenced using APA 7th. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Questions to be answered by the student:** | | **Satisfactory** | | |
| **Yes** ✓ | **No** 🗶 | |
| Q1 | **Name** and **describe** the Australian legislation that pertains to data protection. In you answer, specifically include how this legislation relates to cyber security. |  | |
| **Response:**  The Australian legislation that pertains to this is the Australian Privacy Act of 1988. Within the legislation it talks about 13 Privacy Principles and how they affect the collection and distribution of a citizen’s personal information. This affects cyber security because often, your personal information is the data that websites and services collect and need to protect. These services and websites need to tell you what information they are collecting, what they will do with it and to keep you anonymous. | |  |  |
| Q2 | **Explain** how the Notifiable Data Breach legislation affects organisations and how it links to other Australian legislation. |  | | |
| **Response:**  It affects organisations because under the legislation its states that organisations that have an eligible data breach must inform the OIAC (Office of the Australian Information Commissioner) and all affected individuals when that breach occurs. This links to the legislation from the previous question, the Privacy Act, that determines that anybody, individual or organisation that has access to people’s personal information MUST disclose the management and use of that information, including its mismanagement. | |  |  | |
| Q3 | **Describe** the General Data Protection Regulations (GDPR), its major provisions, and how it relates to Australian entities. |  | | |
| **Response:**  The General Data Protection Regulations is a regulation that protects the personal data of EU citizens, as such it applies to any company/website or application that could and would work in the EU. It gives its subjects the right to correct inaccurate personal information, see how their data is being used and the right to be notified if their data has been breached, and more. Some differences between the 1988 Privacy Policy and the GDPR are that the GDPR regulates that when a person’s data is breached, the holder must inform them of that breach within 72 hours while the Privacy Policy doesn’t have this time requirement. The GDPR also requires explicit consent to collect data while the Australian policy only requires implied consent. | |  |  | |
| Q4 | **List** and **describe** a policy that relates to securely storing, sharing, and managing information. In your answer, include the main provisions and procedures the policy would need to include, giving examples. |  | | |
| **Response:**  Some policies that would relate to the secure storage and managing of data are   * Password Policy and Clean Desk Policy   A password policy states the minimum requirements of different characters and length of a password that can give access to sensitive information. A clean desk policy would state that the desk where you access this information should be well kept and cleanly, to a standard of health and safety. But it would also specifically provision against the writing down of a password on paper and what can be stored within this space.   * Cloud Storage Policy   This type of policy would dictate what can and can’t be stored on cloud storage systems. It would be based on the sensitivity of the data and relate to other policies regarding passwords and encryption to determine if the service/storage is safe enough for that information. | |  |  | |
| Q5 | **List** and **describe** a policy that relates to encryption. In your answer, include the main provisions and procedures the policy would need to include, giving examples. |  | | |
| **Response:**   * Acceptable Encryption Policy   This is a kind of policy that guides what types of encryptions are acceptable within the organisation. It could specify acceptable encryption algorithms, cyphers or even key length. It would determine where and when this encryption should or must be applied when communicating, either between colleagues or entities outside of the organisation like a contractor. | |  |  | |
| Q6 | **List** and **describe** a policy that relates to data classification and management, and media/document labelling. In your answer, include the main provisions and procedures the policy would need to include, giving examples. |  | | |
| **Response:**   * Data Classification Policy   This policy is about how an organisation categorises data. This is usually about sensitivity, so an organisation knows what protections a piece of data requires, if it is only Private or Highly Sensitive. These classifications are usually made by considering the potential effect of that data being maliciously or incorrectly distributed.   * Data Management Policy   This policy dictates the entire life cycle of a piece of data, starting from where it is stored, how it would be organised, how it would be destroyed. Other things it would consider is how many backups of data there would be and how those are managed. How data is shared and accessed within the organisation and with partners or contractors. | |  |  | |
| Q7 | **List** and **describe** a policy that relates to data governance. In your answer, include the main provisions and procedures the policy would need to include, giving examples. |  | | |
| **Response:**   * Data Governance Policy   This policy details how each worker is responsible for the security and quality of data. It would outline each role within the company and the relevant actions and precautions they would need to follow over the lifecycle of a project. This policy is a broad overview of how data is handled specifically within the organisation and by whom. | |  |  | |
| Q8 | **List** and **describe** a policy that relates to acceptable use of workplace equipment. In your answer, include the main provisions and procedures the policy would need to include, giving examples. |  | | |
| **Response:**   * Acceptable Use Policy   As the name implies, an acceptable use policy outlines how the company accepts users to interact with networks, equipment and utilities on or off premises. It would outline the accepted procedure for logging on or using a network and what not to use it for, like personal searches or projects.   * Internet Usage Policy   An internet usage policy is extremely common as most workplaces operate with access to the internet and provide it to their employees for use through private networks. Given that it is paid for and provided by the company, they can restrict what the internet is used for; for example, recreation, internet shopping or viewing inappropriate content. | |  |  | |
| Q9 | **List** and **describe** a policy that relates to bringing your own devices for use in the workplace. In your answer, include the main provisions and procedures the policy would need to include, giving examples. |  | | |
| **Response:**   * Bring Your Own Device (BYOD) Policy   A BYOD Policy governs when, how and if a member of staff can bring their own personal device into work. It focuses on how they will need to connect to the company’s network and how they will use that network. For example, ensuring that the device meets security requirements and potentially if the device needs to be checked and approved by cyber security before it connects to the network. | |  |  | |
| Q10 | **List** and **describe** at least two online Australian government sources you can use to find information on current cyber security threats. For each, include a link to the source. |  | | |
| **Response:**   * The Australian Cyber Security Centre   This is a hub of government approved guides and online resources to keep individuals and company’s up to date on cyber security practices and threats.   * <https://www.cyber.gov.au/> * The Department of Home Affairs   This is a government branch that establishes national security policy and processes. It represents a joined effort by cyber security officials, emergency management and national security forces to name a few. Its website has information relevant to cyber security acts and programs that the government enforces or uses.   * <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/overview> | |  |  | |
| Q11 | **List** and **describe** at least two risks associated with cyber security in the workplace. For each, give an example of the potential harm that it can cause. |  | | |
| **Response:**   * Malware   Malware is malicious software that attempts to harm or damage the system that it is uploaded onto. It can be focused on stealing or destroying systems and their data.   * Phishing   Phishing is the act of tricking someone into revealing personal information through falsified emails or websites. This is usually an attempt to steal someone’s identify or solicit money from them. With the information, the criminals can gain access to personal bank accounts or even company systems depending on what information they take. | |  |  | |
| Q12 | **List** and **describe** two strategies and techniques to improve workplace cyber security, from a technical standpoint. For each, explain what it is and how it helps promote cyber security in the workplace. |  | | |
| **Response:**   * Patching Applications   Ensuring that all applications are up to date with the most recent patches to ensure the most recent vulnerability patches are applied.   * Multi-Factor Authentication   When logging in and accessing confidential information, multi-factor authentication should be applied, meaning that the user must use generated codes and connected fingerprint or facial recognitions to gain access. | |  |  | |
| Q13 | **List** and **describe** two techniques to implement and improve cyber security awareness in the workplace. For each, explain what it is and how it helps promote cyber security in the workplace. |  | | |
| **Response:**   * Reminders   This term is used for casual notices and signage around the office meant to remind staff to obey cyber-security protocols.   * Training   This involves intensive sessions that are meant to teach the staff what they are supposed to do for cyber-security. They can be done semi-regularly and should be administered upon onboarding. | |  |  | |
| Q14 | **List** and **describe** two techniques to facilitate cyber security awareness training in the workplace that include simulated activities. For each, explain what it is and how it helps promote cyber security in the workplace. |  | | |
| **Response:**   * Testing   After going through an induction or training session, employees can be tested on their knowledge to ensure and certify that they understood what was taught. This can also help to find areas where people are confused, or the training material is not sufficient.   * Online Modules   Rather than training in person, online modules can be sent to employees to have them learn and be tested in their own time. This can automate the training process and help to reduce the disruption that regular training sessions may have on working. | |  |  | |