Assessment Task 1: Knowledge Questions

|  |  |
| --- | --- |
| Course code and title | *[Insert Course Code and Title]* |
| Unit code and  title | *[Insert Unit Code and Title]* |
| Due date | Session 5 |
| Resources  required | Learner to provide:  Access to computer and internet  Provided: |
| Decision making rules | To achieve an overall satisfactory result for this assessment task:   * All questions must be answered satisfactorily |
| Learner  instructions | This task is a set of written questions.  For this task you will:  • Complete it individually.  • Complete answers to all questions  • Have time to read and review the assessment task in class.  • Submit your answers electronically via Moodle  If you have any questions about the task or concerns about your ability to complete the task, please discuss this with your Assessor. |

**Knowledge Questions**

| **1** | List 3 Australian federal legislative Acts relevant to cybersecurity and the protection of data. Ensure to include the year of the Act. | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory |  | NOT satisfactory | |
| 1. Criminal Act 1914 2. Surveillance Devices Act 2004 3. Privacy Act 1988 | | | | | | |

| **2** | Using the internet, research the Privacy Act 1988. Based on your research, in one or two paragraphs explain how organisations are expected to treat personal information based on this Privacy Act. | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory |  | NOT satisfactory | |
| The Australian Privacy Act 1988 sets out guidelines for how businesses manage personal data. You should get permission, collect only the information you need, and explain why to others. They must also prevent access and use of data by unauthorized third parties, and individuals can request access to their data and, if necessary, request correction. If you violate these guidelines, your organization risks sanctions. | | | | | | |

| **3** | Outline 2 implications to an organisation if they have a Notifiable Data Breach (NDB). | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory |  | NOT satisfactory | |
| 1. Loss of business data 2. legal costs and court fines | | | | | | |

| **4** | List 5 international standards related to cybersecurity that an organisation can implement and provide an overview of the standard (25-30 words per response). | | | | | |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Answer | |  | Satisfactory |  | NOT satisfactory | |
|  | International Standard | Description | | | | | |
|  | IS0/IEC 27001 | A framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) to protect sensitive data and manage risks. | | | | | |
|  | PCI DSS (Payment Card Industry Data Security Standard) | A set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment to protect cardholder data. | | | | | |
|  | GDPR (General Data Protection Regulation) | A regulation in the European Union (EU) that addresses data protection and privacy for individuals within the EU and the European Economic Area (EEA), focusing on protecting personal data and regulating its processing and movement. | | | | | |
|  | IS0/IEC 27002 | Provides guidelines for establishing, implementing, maintaining, and improving information security management systems by specifying best practices and controls. | | | | | |
|  | CIS Benchmarks | offers best practices for securing IT systems and data against cyber threats, providing configuration guidelines for various operating systems，software, and devices. | | | | | |

| **5** | List 2 Australian government sources of information on current cybersecurity threats. Please provide a web page link to each source in your answer. | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory |  | NOT satisfactory | |
|  | The Australian cyber-Security (entre (ACSC) mission is to lead the Australian government’s efforts to improve cybersecurity within Australia by providing up-to-date advice and information about how to protect individuals and businesses online. Current cybersecurity can be found at:  https://www.cyber.gov.au/acsc/individuals-and-families/threats | | | | | |
|  | The Department of Industry, Science, Energy and Resources has detailed information about Government cybersecurity strategies which can be.  found at:  https://www.industry.gov.au/data-and-publications/australias-tech-future/cyber-security | | | | | |

| **6** | Describe 2 training strategies/techniques that you can use to promote cybersecurity awareness. (20-25 words per response) | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory |  | NOT satisfactory | |
|  | Engage employees in hands-on activities, simulations, and discussions to raise awareness about cybersecurity threats and best practices. | | | | | |
|  | Conduct simulated phishing attacks to educate employees on how to identify and respond to suspicious emails, enhancing their vigilance. | | | | | |

| **7** | Describe 2 techniques apart from employee training that you can use to promote workplace cybersecurity awareness within your organisation. (20-25 words per response) | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory |  | NOT satisfactory | |
|  | Support guides，how-to guides， knowledge bases， and/or wikis. | | | | | |
|  | Cybersecurity signage and posters | | | | | |

| **8** | Explain how you can use simulated activities as part of staff training. Provide an example as part of your answer. (30 -40 words) | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory |  | NOT satisfactory | |
| Employees can immerse themselves in realistic scenarios and practice response measures while identifying vulnerabilities through simulation activities such as network attack scenarios or phishing simulations. For instance, engaging in simulated phishing activities can enhance overall cybersecurity awareness and preparedness by teaching employees how to detect and avoid hazardous emails. | | | | | | |

| **9** | Describe 5 cybersecurity threats and associated risks that an organisation may face. Use the correct industry terminology and briefly describe each cybersecurity threat (20-30 words per response) | | | | | |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory | |  | NOT satisfactory | |
|  | Cloud vulnerabilities | | | threats that target the cloud services that an organisation utilises. | | | |
|  | Denial of Service (Do5) | | | is an attack on an organisations network services designed to either slow down the services that it offers to overwhelm them a11 together causing the services to become unresponsive altogether | | | |
|  | Fake news | | | a form of news consisting of deliberate misinformation, or hoaxes spread via print, broadcast, and/or the Internet, Frou cybersecurity perspective, fake news is spread via webpages and/or social media channels | | | |
|  | Inadequate patch management | | | Is where the organisation has insufficient work processes to ensure that its systems are updated regularly which leaves possible security vulnerabilities that an attacker can exploit | | | |
|  | Credential stuffing. | | | is an automated injection attack where stolen usernames and passwords from a data breach are used to try and gain access to the user accounts on a variety of web applications. | | | |

| **10** | Describe briefly what a BYOD Policy and relevant procedures are designed to achieve. (20-30 words per response) | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory |  | NOT satisfactory | |
| Companies use BYOD policies and related procedures to establish policies and procedures for employees who bring and use personal devices for work. | | | | | | |

| **11** | Describe briefly the purpose of an Acceptable Use Policy and the relevant procedures are designed to achieve. (20-30 words per response) | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory |  | NOT satisfactory | |
| An organization's permitted use policy and related procedures outline the practices and restrictions that guide employees in the proper use of the organization's network and software and indicate what is and is not allowed. | | | | | | |

| **12** | Describe briefly the purpose of an Information Security Policy and the relevant procedures are designed to achieve. (20-30 words per response) | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory |  | NOT satisfactory | |
| Organizations utilize information security policies to protect personal and organizational data. The content and guidelines in this policy relate to secure information storage, sharing and management. These guidelines include when and how to use passwords, encryption, and other security measures. | | | | | | |

| **13** | Describe briefly what an Encryption Policy and relevant procedures are designed to achieve and include 2 examples of when an organisation may ask their staff to use encryption procedures. (20-30 words per response) | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory |  | NOT satisfactory | |
| Sensitive information can be protected during transmission or storage by using encryption strategies to make it uncrackable. Companies may require employees to sign encryption agreements when exchanging private files via email or retaining sensitive data on mobile devices. | | | | | | |

| **14** | Describe briefly why an organisation would implement a procedure to classify data. Include at least 2 classification examples in your answer.  (40 -50 words per response) | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory |  | NOT satisfactory | |
| Organizations will guide employees in classifying data to manage risk. The data is first classified, and then specific procedures can be used for each type of data to protect the types of data that have different values to the company.  For example, organizations can classify data into personal data, customer data, credit data, etc., and then assign different risk levels and different procedures to each type of data. | | | | | | |

| **15** | Describe briefly what a Media/Document Labelling Policy and relevant procedures are designed to achieve. (40 -50 words per response) | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory |  | NOT satisfactory | |
| Media policies and procedures describe the use of removable media.  It includes content and instructions regarding permitted uses and types of removable media, registration processes for removable media, requirements for labelling of removable media, processes for protecting removable media, and how to report lost or stolen removable media. | | | | | | |

| **16** | List and briefly describe 2 further types of policies and relevant procedures that an organisation would implement as part of their data and information governance system for managing data and information assets. | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Answer |  | Satisfactory |  | NOT satisfactory | |
|  | Backup policies and procedures tell employees that data needs to be backed up regularly, either manually or by setting up automatic backup features. Passwords and protocols, helping employees choose very secure passwords or passphrases and how often to update them. | | | | | |
|  | Policies and procedures related to anti-virus and malware software that direct employees to use these programs at specific times or frequencies and provide instructions for their use. | | | | | |

## Assessment Task Summary: Task 1 - Knowledge Questions

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Trainer/Assessor to complete the following:  **THE LEARNER:** | | | | | | Yes | No |
| 1. | Satisfactorily answered all questions. | | | | |  |  |
| feedback **-** Assessor must include feedback | | | | | | | |
|  | | | | | | | |
| OVERALL TASK result | | | | | | | |
| Satisfactory  Not Satisfactory (resubmission required) – Due date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | |
| Date Assessment Returned | | |  | | | | |
| Trainer/assessor Name | | |  | | | | |
| Trainer/Assessor signature | | | X | | | | |
| **LEARNER DECLARATION**: Please read and sign below | | | | | | | |
| I, \_\_WangYiZhuo\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ have been advised of the outcome of this assessment task.  PRINT NAME | | | | | | | |
| LEARNER Signature | | WangYiZhuo +S1554654 | | Date |  | | |