|  |  |
| --- | --- |
| Assessment Title | Knowledge Questions Assessment |

## Competency Details

|  |  |
| --- | --- |
| Unit code/s and title/s | BSBXCS402 Promote workplace cyber security awareness and best practices |
| Qualification code/s and title/s | ICT50220 Diploma of Information Technology |
| Business unit/Work group | Business and Arts/IT Studies |

## Instructions

|  |  |
| --- | --- |
| Method/s of assessment | Questioning (Written) |
| Overview of assessment | This assessment will require you to complete written answers for questions on the tasks listed below. |
| Task/s to be assessed | In this assessment you will be researching aspects of the following topics:   * Legislative and regulatory requirements * Organisational policy and procedures * Cyber sources and strategies |
| Time allowed | Refer to your schedule for submission dates |
| Location of assessment | Assessment can be completed anywhere with access to the resources required (see Resources Required section below) |
| Decision making rules | To receive a satisfactory outcome for this assessment you must complete all parts correctly.  Word counts are provided as guidance only. |
| Assessment conditions | This assessment must be undertaken where the conditions replicate noise levels and interruptions that people typically experience working in the ICT industry.  This is unsupervised assessment and you may access any required resources.  This is not group work and must be completed as an individual. |
| Resources required | To complete this assessment, you will require the following:   * Access to Learn with Internet access * Learn resources * Word processing software such as Microsoft Word. |
| Result notification and reassessment information | You will be provided feedback and the result for your assignment on TAFESA Learn. You will be and given the chance to resubmit with required corrections only once.  Refer to the TAFE SA assessment policy for more information <https://www.tafesa.edu.au/apply-enrol/before-starting/student-policies/assessment> |

## Task 1: Legislative and regulatory requirements

Question 1

List the legislation associated with data protection in cybersecurity and its purpose (approx. 25 words).

* Privacy Act 1988
  + The Privacy act of 1988s purpose is to protect the information of individuals that is stored by government agencies and some private sector organisation.

Question 2

What will be the legal issues that the organisation has to face if data is breached? (approx. 40-80 words).

* Report to authorities notifiable breach of data OAIC and affected parties
* Fines and penalties

Question 3

ITWorks is an organisation which provides various ICT services to their clients. They sell their services over the internet, and customers pay using their credit card. ITWorks keeps a record of the credit card and personal details of the customers on the database. The database used by ITWorks is not secure, and anyone can access it. ITWorks has not implemented a privacy policy or data protection policy.

Recently, there was a cyberattack on ITWorks and as a result credit card and personal details of the customers were taken. Customers are reporting to the organisation that money has gone missing from their accounts.

After reading this case study, Answer the following:

* What legal obligations may ITWorks face?
* What laws have been breached in this scenario?
* Notifying affected individuals
* APP 11.1-11.2 have been breached mainly surrounding the assurance of security of data.

Question 4

List 5 international legislations associated with cybersecurity.

* Cyber crime act 2001
* EU Cybersecurity Act
* Network and Information Security directive
* Criminal code Canada
* GDPR

## Task 2: Organisational policy and procedures

Question 5

a) Match the organisational policies and procedures with the correct work type:

|  |  |
| --- | --- |
| **Organisational policies and procedures** | **Work type** |
| Data protection policy | Securely storing, sharing and managing information and Media/document labelling |
| Bring your device policy (BYOD policy) | Data classification and management |
| Acceptable use policy | Data classification and management |
| Data management policy | Data governance |
| Information management policy | Acceptable use |
| Data governance policy | Bring your device |

Use the table below to complete the task.

|  |  |
| --- | --- |
| **Organisational policies and procedures** | **Work type** |
| Data protection policy | Data classification and management |
| Bring your device policy (BYOD policy) | Bring your device |
| Acceptable use policy | Acceptable use |
| Data management policy | Data classification and management |
| Information management policy | Securely storing, sharing and managing information and Media/document labelling |
| Data governance policy | Data governance |

b) Briefly explain all the policies identified in the table above (approx. 50 – 100 words total)

* Data protection policy
* Bring your device policy (BYOD policy)
* Acceptable use policy
* Data management policy
* Information management policy
* Data governance policy

## Task 3: Cyber sources and strategies

Question 6

List 5 sources of information used by the Australian government to collect information about cyber threats.

* Australian Cyber Security Centre
* Commonwealth fraud control centre
* Australian Public Service Commission
* Australian Security Intelligence Organisation
* Department of Finance.

Question 7

a) List 5 types of risk associated with cybersecurity in the workplace.

* Phishing attack
* Weak password
* Ransomware
* Malware
* Hacking

b) Briefly explain the following risks (approx. 25 words total):

* Phishing attack
* Weak password
* Phishing attacks are attacks through emails or texts that try to steal personal information like passwords and credit cards.
* Weak passwords can be easily guessed, or brute forced, allowing malicious actors to gain access to accounts.

Question 8

Explain the 3 ways below to promote cybersecurity awareness in the workplace (approx. 80 - 100 words total):

* Provide security awareness training:
* Provide training seminars every 3-6 months to make sure workers are up to date on security.
* Encourage the use of strong passwords:
  + Force the use of a password manager that automatically generated passwords making secure and unique passwords for each account, also implementing policies that change passwords every 90 days.
* Document security policies:
  + Security policies should make clear guidelines for staff to follow when handling documents, such as never leaving a device open with the documents available.

Question 9

List 3 guidelines involved in the implementation of cybersecurity awareness.

* Regular training and retraining of staff
* Create simulated attacks to make sure staff are aware of attacks
* Use microlearning with staff

Question 10

List any three practices that can be used to train employees about cybersecurity. One of the practices must include a simulated example.

* Seminars
* Role plays and simulated attacks
* Awareness posters