**Knowledge Questions Assessment**

1. What is sensitive data? Explain how to identify sensitive data in a workplace.

Sensitive data is any data that needs to be protected from unauthorised access. To identify sensitive data in a workplace you must consider the following when collecting information:

* Can the unauthorised party use the information to harm the organisation’s operations, individuals, or assets because of data disclosure or misuse?
* Would the unauthorised disclosure of the data or elements of the data violate any Australian or relevant laws or regulations?
* What would be the likely impact of unauthorised access to the data?
* Would this unauthorised access damage the company’s reputation and public confidence?

1. What are the 7 principles of the General Data Protection Regulation (GDPR)?

* Lawfulness, fairness, and transparency
* Purpose limitation
* Data minimisation
* Accuracy
* Storage limitation
* Integrity and confidentially
* Accountability

1. When must an organisation or agency notify affected individuals and the Office of the Australian Information Commissioner (OAIC) according to Notifiable Data Breach legislation and Privacy Act 1988?

They must notify the affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved. The notification to individuals must include recommendations about the steps they should take in response to this data breach.

1. Explain why securing personally identifiable information (PII) is a critical data protection task.

Securing PII is a critical data protection task because if unauthorised parties obtain PII they can use it to damage the company’s reputation by weakening the trust consumers have in the company which makes customer retention and acquisition much harder. There also may be legal repercussions in a data breach. These unauthorised parties can also make a profit from the data or even steal individual’s identities.

1. What are the uses of encryption?

Data Protection for Storage: It can be used to protect the data stored for a long time. Even if the storage is stolen or breached, the data will still be unreadable without the key.

Data Migration: When transferring data via a network, it is used to ensure that no one in the network can read it.

Accessing Data Across Multiple devices: Data stored on cloud storage is Encrypted, and it can then be accessed from any supported device securely.

Ensuring Compliance: Considering the value of data security, many organizations, governments, and companies require the data to be secured with Encryption to keep the company or user data safe. This also prevents employees from having unauthorized access to user data.

1. What is the difference between data deletion and data erasure?

Data deletion leaves data recoverable, while data erasure is permanent; this is especially important for businesses, as getting these two terms confused can present significant issues.

1. What are the risks of communicating sensitive information via email and SMS?

Identify four (4) types of information that should never be shared via email or SMS?

The risks with communicating sensitive information via email and SMS is the information is insecure, the data is then being stored on your PC/Phone, therefore you no longer control the sensitive data. The 4 types of information that should never be shared via email or SMS are business information (financial statements, accounting data, bank account information), customer information (names, addresses, payment information), employee data (usernames and passwords, payment information), intellectual property (competitive research, product specifications).

1. What are four (4) risks and four (4) benefits associated with cloud storage?

Risks: data privacy, lack of control, shared servers, APIs and storage gateways

Benefits: easy disaster recovery, access your data anywhere, low cost, security