Data Security Short Response Practice

Question 1

Explain the three core principles of cybersecurity, known as the CIA Triad, and provide a brief example for each. [6 marks]

Question 2

Differentiate between symmetric encryption and asymmetric encryption, outlining a primary advantage and use case for each method. [6 marks]

Marking Guide

#	Sample Response	Response	Mark
1	The CIA Triad comprises three core principles of cybersecurity: Confidentiality, Integrity, and Availability. Confidentiality ensures that only authorized individuals can access specific data, preventing it from being read or stolen by unauthorized parties. An example is encrypting messages sent through WhatsApp so that only the intended recipient can read them, even if intercepted. Integrity ensures that data remains correct, complete, and unaltered unless changed in an authorized way, protecting against tampering, accidental deletion, or corruption. An example is software updates being digitally signed by developers to assure users that the file has not been altered by hackers. Availability ensures that authorized users can always access their systems and data when needed, defending against attacks that stop people from using services. An example is a bank's website being accessible 24/7 for customers to check their accounts.	Explains confidentiality	1
		Provides confidentiality example	1
		Explains integrity	1
		Provides integrity example	1
		Explains availability	1
		Provides availability example	1
2	Symmetric encryption uses a single secret key for both encrypting and decrypting electronic information. Parties communicating must securely exchange this key. A primary advantage is that it is faster and more efficient for encrypting large amounts of data, such as entire databases. Examples include AES, DES, and Blowfish. Asymmetric encryption (also known as public-key cryptography) uses two distinct keys: a public key for encryption and a private key for decryption. The public key can be freely distributed, while the private key is kept secret. A primary advantage is that it simplifies key distribution and enhances security by ensuring the private key is never shared. It is commonly used for secure online communication and digital signatures. Examples include RSA and Diffie-Hellman Key Exchange.	Explains symmetric encryption	1
		Explains symmetric encryption advantage	1
		Provide symmetric encryption example	1
		Explains asymmetric encryption	1
		Explains asymmetric encryption advantage	1
		Provide asymmetric encryption example	1