Helwan University
Faculty of Computers and Information
Department: Computer and Information
Course: Network Security
Midterm Exam
Duration: 1 Hour **Total Marks:** 40

Section A: Multiple Choice Questions (10 Marks)

Instructions: Circle the most correct answer for each question. *(1 Mark each)*

1. The C.I.A. triad, which is now often considered a base for a more expanded model, consists of:
   a) Confidentiality, Integrity, Accountability
   b) **Confidentiality, Integrity, Availability**
   c) Confidentiality, Integrity, Authentication
   d) Control, Integrity, Availability

2. The person in an organization with primary responsibility for the assessment, management, and implementation of InfoSec is the:
   a) CIO b) CEO **c) CISO** d) Data Custodian

3. Which of the following is defined as *"a potential weakness in an asset or its defensive control system(s)"*?
   a) Threat b) Attack **c) Vulnerability** d) Exploit

4. A coordinated stream of requests launched against a target from many locations simultaneously is known as a:
   a) Denial-of-Service (DoS) attack
   b) Phishing attack
   c) Distributed Denial-of-Service (DDoS) attack
   d) Man-in-the-Middle attack

5. Which approach to implementing information security is initiated by upper management, involves issuing policies, and is generally the most successful?
   a) Bottom-Up Approach b) Grassroots Approach c) Ad-Hoc Approach **d) Top-Down Approach**

6. An individual appointed by data owners to oversee the management of a particular set of information and coordinate with data custodians is known as a:
   a) Data User **b) Data Trustee** c) Data Owner d) CIO

7. Which of the following techniques uses social skills to convince people to reveal access credentials?
   a) Pharming b) Sniffing **c) Social Engineering** d) Spoofing

8. The quality or state of preventing disclosure or exposure to unauthorized individuals or systems is known as:
   a) Integrity b) Availability c) Utility **d) Confidentiality**

9. Which category of threat includes power shortages, ISP failures, and other service disruptions?
   a) Forces of Nature **b) Deviations in Quality of Service** c) Technological Obsolescence d) Technical Hardware Failures

10. Which of the following is **NOT** typically considered a communications interception attack?
    a) Packet Sniffing b) IP Spoofing **c) Ransomware** d) Man-in-the-Middle

---

Section B: True/False Questions (5 Marks)

Instructions: Write *(T)* for True or *(F)* for False in the space provided. *(1 Mark each)*

( ) Information security began as a field immediately after the development of the first mainframes.
( ) A “script kiddie” is an expert hacker who develops their own sophisticated attack software.
( ) A breach of possession always results in a breach of confidentiality.
( ) The primary mission of an information security program is to ensure that information assets remain safe and useful.
( ) In a top-down approach to security implementation, systems administrators lead the grassroots effort.

Section C: Short Answer Questions (15 Marks)

Instructions: Answer the following questions concisely.

1. **List the three core objectives of the C.I.A. triad and provide a brief definition for each.** *(3 Marks)*
   a)
   b)
   c)

2. **Define the following terms:** *(4 Marks)*
   a) Threat:
   b) Attack:
   c) Vulnerability:
   d) Exploit:

3. **Name any four roles that can be part of an Information Security Project Team.** *(4 Marks)*
   a)
   b)
   c)
   d)

4. **List four of the twelve general categories of threats to information security.** *(4 Marks)*
   a)
   b)
   c)
   d)

Section D: Scenario-Based / Essay Question (10 Marks)

Instructions: Answer the following question in a short paragraph.

A small but growing e-commerce company is experiencing rapid success. The CEO believes that security is “holding the business back” and that developers should focus solely on adding new features to the website, even if it means delaying security updates.

Question:
Based on what you have learned, discuss the importance of information security for this company. In your answer, explain at least **two key functions** of information security and **one potential threat** the company might face if it neglects security. Conclude by explaining the concept of balancing business needs with security needs.

Answer Key

Section A: Multiple Choice

1. b 2. c 3. c 4. c 5. d 6. b 7. c 8. d 9. b 10. c

Section B: True/False

T F F T F

Section C: Short Answer

1.

a) **Confidentiality:** Prevention of unauthorized disclosure.
b) **Integrity:** Protection against unauthorized modification; ensures accuracy and completeness.
c) **Availability:** Ensures authorized users have timely and reliable access to information.

2.

a) **Threat:** A potential risk of harm to an asset.
b) **Attack:** An intentional or unintentional act that damages or compromises information/systems.
c) **Vulnerability:** A weakness in a system or its defenses that can be exploited.
d) **Exploit:** A technique or tool used to compromise a system via a vulnerability.

3. *(Any four of the following)* — Champion, Team Leader, Security Policy Developers, Risk Assessment Specialists, Security Professionals, Systems Administrators, End Users.

4. *(Any four of the following)* — Compromises to intellectual property, Deviations in quality of service, Espionage or trespass, Forces of nature, Human error or failure, Information extortion, Sabotage or vandalism, Software attacks, Technical hardware failures or errors, Technical software failures or errors, Technological obsolescence, Theft.

Section D: Sample Essay Answer

Information security is crucial for the e-commerce company's survival and growth. Its primary functions include protecting the organization's ability to operate by ensuring that its website and payment systems remain available, and protecting sensitive customer data such as payment details and personal information. Neglecting security exposes the company to threats like ransomware attacks that could encrypt critical databases, disrupt services, and damage its reputation. While business expansion is important, achieving a balance between business and security needs is essential. Integrating security into the development process ensures sustainable growth, operational stability, and customer trust.