Daffodil International University
Faculty of Business and Entrepreneurship
Department of Business Administration
Program: BBA

Semester: Spring-2025
Time: 2 hours
Course Code: 0613-223
Section: 65 (A, B, C, D, E, F, G)
MFH

Examination: Final
Full Marks: 40
Course Title: Cyber Security for Business
Teacher's Name: MI/FK/ MAI/ RT/ FC/

Instructions:

1. **Answer all the questions.**
2. **Any kind of unfair means is strictly prohibited.**
3. **Read the question attentively, then answer to the point; relevant examples will carry greater marks.**

[Marks: 10]

Question No. 1: [CLO 2, Level 4]

Suppose you are the Incident Response (IR) Manager for a large e-commerce company that recently experienced a security breach. A sophisticated cyberattack has compromised several of the company's web servers, and attackers have gained unauthorized access to sensitive customer data, including credit card details and personal information. The incident involves not only a data breach but also potential reputational damage, customer trust issues, and compliance violations related to privacy regulations like GDPR and PCI-DSS.

As the Incident Response Manager, **discover** the detailed incident response lifecycle steps for this company that will help eradicate losses.

[Marks

Question No. 2: [CLO 3, Level 3]

5+5=10]

You are the Chief Information Security Officer (CISO) at a mid-sized organization. The company is implementing a new policy to ensure data protection and privacy for its employees and customers. The organization collects and processes personal data (such as emails, payment details, and customer preferences) as part of its operations. Recently, there have been increased concerns about cyber-attacks, and the company is also receiving more scrutiny from regulatory bodies about compliance with privacy laws such as GDPR and CCPA

As part of your role, **Identify** and explain best practices for data protection and privacy, focusing on both individuals and organizations.

[Marks: 10]

Question No. 3: [CLO 3, Level 3]

You are the Chief Executive Officer (CEO) of a multinational company that recently experienced a data breach due to an employee falling for a phishing attack. Investigations revealed that cybersecurity awareness among employees was low, and there was no clear security culture within the organization. Stakeholders, including board members and customers, are now concerned about the company's commitment to cybersecurity.