The Open University of Sri Lanka
Faculty of Engineering Technology
Department of Electrical & Computer Engineering

Study Programme	:	Bachelor of Science Honours in Engineering
Name of the Examination	:	Final Examination
Course Code and Title	:	**EEX5270- Information Security**
Academic Year	:	2024/25
Date	:	17th February 2026
Time	:	09.30-12.30h
Duration	:	3 hours

General instructions

1. Read all instructions carefully before answering the questions.
2. This question paper consists of **Four (4)** questions in **Two (2)** pages.
3. Answer **all** questions.
4. Answer for each question should commence from a new page.
5. This is a Closed Book Test (CBT).

Question 01 [25 Marks]

a) Explain the fundamental role of the CIA model (Confidentiality, Integrity, and Availability) in safeguarding information systems and organizational data. (10 Marks)

b) Using practical or real-world scenarios, demonstrate how failures in each of these three security principles may occur and analyze the possible impacts on individuals or organizations. (8 Marks)

c) Evaluate the effects of common cyber threats such as ransomware attacks, malicious insiders, and denial-of-service incidents on Confidentiality, Integrity, and Availability. (7 Marks)

Question 02 [25 Marks]

a) Describe the role of cryptographic techniques in protecting digital information. In your answer, explain the concept of encryption and compare secret-key cryptography and public-key cryptography, illustrating their practical applications in modern information systems. (10 Marks)

b) Explain the access control concept known as the principle of least privilege. Analyze how this principle reduces the attack surface within an organization and describe common methods used to enforce it. (8 Marks)

c) Human factors play a major role in cybersecurity incidents. Discuss how staff education and security awareness programs contribute to reducing cyber threats and strengthening an organization's overall security posture. (7 Marks)

Question 03 [25 Marks]

a) Analyze the potential security and operational challenges faced by healthcare organizations when the principles of Confidentiality, Integrity, and Availability are inadequately implemented in digital health systems. In your answer, consider the impact on electronic medical records, patient privacy, and continuity of clinical services. (10 Marks)

d) Define and discuss the importance of the following information security concepts in the context of protecting organizational systems and data: (8 Marks)

i. Security vulnerability

ii. Risk

iii. User authentication

iv. Access authorization

c) User identity verification plays a vital role in securing information systems. Examine the primary categories of authentication mechanisms, explaining how each method contributes to secure access control. (7 Marks)

Question 04 [25 Marks]

a) Explain how organizations handle cybersecurity risks as part of their overall security strategy. In your answer, describe common risk treatment options and justify why each approach is important for maintaining business continuity and resilience. (10 Marks)

b) Web applications are frequent targets of cyberattacks. Describe the mechanism of a SQL Injection attack that exploits improper input validation, and analyze the possible consequences for application functionality, data integrity, and end users. (8 Marks)

c) Secure software development practices emphasize early detection of weaknesses. Discuss the benefits of incorporating security considerations from the initial stages of the software development life cycle (SDLC), with reference to cost efficiency, risk reduction, and system robustness. (7 Marks)