00032

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

Study Programme	:	Bachelor of Science Honours in Engineering
Name of the Examination	:	Final Examination
Course Code and Title	:	**EEX5270 - Information Security**
Academic Year	:	2023/2024
Date	:	5th March 2025
Time	:	9.30 am - 12.30 pm
Duration	:	3 hours

General instructions

1. This question paper contains four (04) questions. Answer all questions.
2. Closed book Exam.
3. Please remember to write your registration number in the space provided above and in the answer script. **Do not write your name.**
4. In case of doubt, consult the supervisor or an invigilator conducting the examination.

Question 1 (25 Marks)

1. Discuss the significance of the CIA Triad (Confidentiality, Integrity, and Availability) in information security. (10 Marks)

2. Provide real-world examples illustrating how each of the above principles can be compromised and the potential consequences. (8 Marks)

3. Discuss how security threats such as ransomware, insider threats, and denial of service attacks impact each of these principles. (7 Marks)

Question 2 (25 Marks)

1. Discuss the risks of not ensuring the CIA (Confidentiality, Integrity, and Availability) in a Healthcare Information System. Highlight potential consequences and vulnerabilities related to electronic health records (EHR), patient data security, and healthcare service delivery. (10 Marks)

2. Explain the significance of the following cybersecurity terminologies and their roles in ensuring information security. (8 Marks)

    i. Vulnerability
    ii. Risk
    iii. Authentication
    iv. Authorization

3. Authentication is a critical aspect of cybersecurity. Discuss the three main forms of authentication, providing a detailed explanation of each. (7 Marks)

Question 3 (25 Marks)

1. Encryption is a critical component of cybersecurity, ensuring data confidentiality and protection. Define encryption and differentiate between symmetric and asymmetric encryption with practical examples of their usage. (10 Marks)

2. Explain the principle of least privilege in the context of information security. Discuss its significance in minimizing security risks and how it is implemented in organizations. (8 Marks)

3. Discuss the importance of employee training and awareness in preventing cyberattacks. How does a well-informed workforce contribute to an organization's overall cybersecurity posture? (7 Marks)

Question 4 (25 Marks)

1. Risk management is a critical aspect of cybersecurity and organizational resilience. Discuss key risk response strategies, explaining their significance. (10 Marks)

2. SQL injection attack is considered to be web-based attacks. Provide an overview of how this attack operates and its potential impact on web applications and users. (8 Marks)

3. Discuss how identifying and addressing security vulnerabilities early in the software development process enhances overall security, reduces costs, and ensures the deployment of robust and secure applications. (7 Marks)

.....