UNIVERSITY EXAMINATIONS

EXAMINATION FOR JANUARY-APRIL 2023/2024 FOR DIPLOMA IN CYBER SECURITY AND DIPLOMA IN ETHICAL HACKING

RES 029: INFORMATION SECURITY MANAGEMENT SYSTEM

DATE: _____ **TIME: 2 HOURS**

GENERAL INSTRUCTIONS:

Students are NOT permitted to write on the examination question paper during exam time.

This is a closed book examination. Text book/Reference books/notes are not permitted.

SPECIAL INSTRUCTIONS:

This examination paper consists Questions in Section A followed by section B.

Answer **Question 1 and any Other Two** questions.

QUESTIONS in ALL Sections should be answered in answer booklet(s).

1. **PLEASE start the answer to EACH question on a NEW PAGE.**
2. **Keep your phone(s) switched off at the front of the examination room.**
3. **Keep ALL bags and caps at the front of the examination room and DO NOT refer to ANY unauthorized material during the course of the examination.**
4. **ALWAYS show your working.**
5. **Marks indicated in parenthesis i.e. ( ) will be awarded for clear and logical answers.**
6. **Write your REGISTRATION No. clearly on the answer booklet(s).**
7. **For the Questions, write the number of the question on the answer booklet cover page in the order you answered them.**
8. **DO NOT use your PHONE as a CALCULATOR.**
9. **YOU are ONLY ALLOWED to leave the exam room 1hour to the end of the Exam.**
10. **DO NOT write on the QUESTION PAPER. Use the back of your BOOKLET for any calculations or rough work.**

SECTION A (Compulsory)

Question One (30 marks)

a. State **THREE** importance of conducting a risk assessment when developing security policies

(3 Marks)

b. What is the primary role of encryption in information security?

(1 Mark)

c. Which component of the CIA Triad ensures that data remains unaltered and trustworthy during storage, transmission, and processing?

(1 Mark)

d. Discuss the following terms as used in information Security

(5 Marks)

i. Information security
ii. Cryptographic key
iii. Cipher text
iv. Encryption
v. Decryption

e. Discuss **TWO** roles of public key infrastructure (PKI).

(4 Marks)

f. Explain **TWO** types of Encryption keys giving at least one example in each

(6 Marks)

g. Discuss the importance of collaborating with external entities, such as vendors and law enforcement, during incident response.

(4 Marks)

h. Name **ONE** of the key components of incident response that focuses on understanding what happened during an incident.

(1 Mark)

i. Define SQL injection and explain **TWO** methods to mitigate it through secure coding practices.

(5 Marks)

SECTION B (Answer Any Two questions: Total: 40 Marks)

Question Two (20 Marks)

a. Explain **FOUR** Reasons why Risk Management is important in Today's Business Landscape

(8 Marks)

b. Discuss **THREE** types of risk responses in the context of risk management.

(6 Marks)

c. Explain **THREE** significant ways in which authentication contributes to the overall security of the online banking platform and how these measures can safeguard sensitive financial information

(6 Marks)

Question Three (20 Marks)

a. At Riara University, Information system users have been categorized into students, Lecturers and admin (ICT department). Students have been given read-only access, The Lecturer can read and modify data while the admin has full control. Explain **THREE** benefits of this categorization.

(6 Marks)

b. Explain **THREE** advantages of utilizing Intrusion Prevention Systems (IPS) over Intrusion Detection Systems (IDS)

(6 Marks)

c. Discuss **FOUR** significance of user training and awareness as one of the steps in creating effective security policies.

(8 Marks)

Question Four (20 Marks)

a. Explain **THREE** types of security policies giving example in each

(6 Marks)

b. Outline **THREE** basic characteristics of information security and detail practical measures for the implementation of each characteristic

(6 Marks)

c. Imagine Tony is an IT security manager for a healthcare organization that handles patient medical records. Explain how implementing data encryption in transit can help the organization where Tony works to comply with privacy regulations and protect sensitive patient data.

(8 Marks)

Question Five (20 Marks)

Case Study: Security Incident Response in a Healthcare Organization

HealthCareSecure, a prominent healthcare organization that manages patient medical records, is committed to ensuring data security and privacy. They've recently faced a security incident involving a significant data breach, which has exposed sensitive patient information. HealthCareSecure's incident response team has been activated to manage the situation. Approximately two weeks ago, HealthCareSecure's security team noticed unusual network activity and confirmed that an unauthorized entity had gained access to patient records. The breach compromised personal and medical data, putting the organization at risk of non-compliance with stringent data protection regulations. Patient trust and the organization's reputation are also on the line.

a. What are the critical steps that HealthCareSecure should take during the initial identification and containment phases of this security incident?

(6 Marks)

b. Explain the roles and responsibilities of key team members within HealthCareSecure's incident response team during the response phase. How does effective collaboration among team members, including IT staff, legal, and management, contribute to mitigating the incident and ensuring a successful response?

(6 Marks)

c. Describe the importance of incident recovery testing and the benefits it can offer HealthCareSecure in terms of improving their incident response procedures and overall data security.

(8 Marks)