JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR DIPLOMA IN CYBER SECURITY

2nd Year 1st SEMESTER 2024/2025 ACADEMIC YEAR

MAIN REGULAR

COURSE CODE: ISD 1203

COURSE TITLE: CYBER SECURITY SYSTEM INSTALLATION

EXAM VENUE: **STREAM: (DIP. CYBER SECURITY)**

DATE: **EXAM SESSION: SEPT – DEC 2024**

TIME: 2.00 HOURS

Instructions:

This paper consists of two sections A and B

i. Attempt **ALL** questions in section A and any **THREE** in section B
ii. Candidates are advised not to write on the question paper.
iii. Candidates must hand in their answer booklets to the invigilator while in the examination room.

SECTION A (40 MARKS)

(Answer All questions in this section)

1. Define Sensitive Data and explain why it is crucial for organizations to protect it. (4 Marks)
2. Identify and explain the different types of sensitive data that organizations must safeguard, providing examples for each. (4 Marks)
3. What are the potential consequences for organizations failing to protect Personal Identifiable Information (PII)? Provide at least two real-world examples. (4 Marks)
4. Discuss the role of Intellectual Property (IP) in business operations and explain why unauthorized access or disclosure can cause significant harm. (4 Marks)
5. What is Protected Health Information (PHI), and why is it critical for healthcare organizations to protect it? Explain the legal framework governing PHI protection. (4 Marks)
6. What are the implications of failing to protect Payment Card Industry (PCI) data for an organization? Mention the key standards that govern PCI data protection. (4 Marks)
7. What are the key considerations organizations should keep in mind when researching and selecting appropriate security solutions? (4 Marks)
8. Explain the concept of security architecture. What are the key components of a well-designed security architecture for an organization? (4 Marks)
9. Describe the steps involved in designing security controls that align with compliance standards such as ISO 27001 or PCI-DSS. (4 Marks)
10. Why is it essential to develop a detailed implementation plan when deploying security solutions? List at least three critical components of an implementation plan. (4 Marks)

SECTION B (60 MARKS)

(Answer ANY THREE questions from this section)

11. (a)Describe the process and significance of conducting vulnerability assessments within an organization. Include tools and methods typically used. (10 Marks)
    (b) Explain how penetration testing complements vulnerability assessments in strengthening an organization's cybersecurity posture. Provide examples of penetration testing techniques. (10 Marks)
12. (a) Discuss the role of Security Information and Event Management (SIEM) tools in monitoring system performance and security. Highlight their key features. (10 Marks)
    (b) Explain the steps involved in responding to performance anomalies, including detection, mitigation, and communication during an incident. (10 Marks)
13. (a)Outline the essential components that should be included in a system installation report, focusing on hardware and software configurations. (10 Marks)
    (b) Discuss the importance of documenting deviations from the original installation plan and how these records contribute to future projects. (10 Marks)

14. You are tasked with establishing a security system for a mid-sized organization facing increasing cyber threats. Write an essay detailing the process of researching and selecting appropriate security solutions, designing a robust security architecture, and planning the implementation steps. (20 Marks)