JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY SECURITY AND AUDIT

1ST YEAR 1st SEMESTER 2024/2025 ACADEMIC YEAR

KISUMU CAMPUS

MAIN PAPER

COURSE CODE: ICM 1102

COURSE TITLE: ADVANCED INFORMATION SYSTEM SECURITY

EXAM VENUE: **STREAM:**

DATE: **22/4/2025** **EXAM SESSION: 14.00-17.00**

TIME: 3 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION ONE (20 marks)

a) Explain the significance of the CIA Triad in information security and provide real-world examples illustrating its application. (10 marks)
b) Discuss the difference between security threats, vulnerabilities, and attacks, giving relevant examples for each. (10 marks)

QUESTION TWO (20 marks)

a) Compare and contrast security policies, procedures, and standards, highlighting their importance in organizational security. (10 marks)
b) Discuss the role of international security standards (e.g., ISO/IEC 27001, NIST Cybersecurity Framework) in enhancing information security. (10 marks)

QUESTION THREE (20 marks)

a) Describe the risk management process in information security and explain the importance of conducting a risk assessment. (10 marks)
b) Differentiate between qualitative and quantitative risk analysis, providing examples of their application in cybersecurity. (10 marks)

QUESTION FOUR (20 marks)

a) Explain the six phases of the incident response lifecycle and their role in mitigating security incidents. (10 marks)
b) Discuss the key components of a Disaster Recovery Plan (DRP) and explain their significance in ensuring business continuity. (10 marks)

QUESTION FIVE (20 marks)

a) Discuss key network security measures such as firewalls, VPNs, and intrusion detection systems, explaining their role in protecting data. (6 marks)
b) Analyze the importance of security awareness training in preventing cyber threats and discuss methods used to educate employees. (6 marks)
c) Discuss the challenges organizations face in implementing effective security awareness programs and suggest ways to overcome them. (8 marks)