JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE IN BUSINESS INFORMATION SYSTEM

4TH YEAR 2ND SEMESTER 2023/2024 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ITB 1404

COURSE TITLE: FUNDAMENTALS OF INFORMATION SYSTEM SECURITY AND POLICY

EXAM VENUE: CL II **STREAM:**

DATE: 22/04/2024 **EXAM SESSION: 9.00 – 11.00 AM**

TIME: 2 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 [30 MARKS]

a) Define information security. 2 marks

b) Explain Five significance of information security in modern organizations? 5 marks

c) Differentiate between threats, vulnerabilities, and risks in the context of information security. 3 marks

d) Describe the components of a risk management framework (e.g., identify, assess, mitigate, monitor) and explain how it helps organizations proactively manage security risks. 8 marks

e) State and explain Six significance of security awareness and training programs in promoting a culture of security within an organization. 6 marks

f) Discuss Four roles of incident response teams between different stakeholders during incident response activities. 4 marks

g) Describe any two methods for encrypting data-in-transit to protect sensitive information from unauthorized access. 2 marks

QUESTION TWO [20 MARKS]

a) Discuss the CIA triad (Confidentiality, Integrity, Availability) and its relevance to information security. Provide and explain **THREE** examples in each case of how each aspect is implemented in an organization's security policies. 12 marks

b) Describe **FOUR** alternative authentication methods other than password-based authentication 8 marks

QUESTION THREE [20 MARKS]

a) State and explain the **SIX** potential consequences of data breaches and privacy violations for organizations? 12 marks

b) What is data-at-rest, describe the **THREE** methods for encrypting data-at-rest to protect sensitive information from unauthorized access. 8 marks

QUESTION FOUR [20 MARKS]

a) Define identity and authentication in the context of information security. What are the **FOUR** common authentication factors, and how do they contribute to user authentication? 10 marks

b) Discuss the importance of regulatory compliance and industry standards (e.g., GDPR, ISO 27001) in shaping security policies. How do these standards influence organizational security practices? 10 marks

QUESTION FIVE [20 MARKS]

Describe the purpose and function of security controls in protecting information systems. Provide examples of administrative, technical, and physical controls. 20 marks