MURANG'A UNIVERSITY OF TECHNOLOGY

SCHOOL OF COMPUTING AND INFOMRATION TECHNOLOGY

DEPARTMENT OF INFOMRATION TECHNOLOGY

UNIVERSITY ORDINARY EXAMINATION

2024/2025ACADEMIC YEAR

FOURTH YEAR **FIRST** SEMESTER EXAMINATION FOR BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

SIT 403: SYSTEM SECURITY AND AUDIT

DURATION: 2 HOURS

INSTRUCTIONS TO CANDIDATES:

1. Answer question ONE and any other two questions.
2. Mobile phones are not allowed in the examination room.
3. You are not allowed to write on this examination question paper.

SECTION A – ANSWER ALL QUESTIONS IN THIS SECTION

QUESTION ONE (30 MARKS)

a) Briefly discuss the information System security ”CIA” Traid. (6 marks)

b) Mwangaza Sacco Ltd is a Sacco operating in Kenya. Recently the Kenyan Government agency that oversees Sacco operations in Kenya (SARSA), emphased on the need to heighten IT Security in all Sacco. Mwangaza SACCO LTD. has invited you to conduct a comprehensive system audit for which IT security plans will be drawn. Evaluate four areas that you intend to audit and briefly explain the reason. (8 marks)

c) Evaluate the importance of capturing network traffic for the purpose of auditing systems. (6 marks)

d) Illustrate why cyber-crime management is increasingly becoming a difficult task for various enterprises to handle. (6 marks)

e) Assess two benefits of using Kerberos as in authentication method between clients and servers. (4 marks)

SECTION B– ANSWER ANY TWO QUESTIONS IN THIS SECTION

QUESTION TWO (20 MARKS)

a) Define the term Cyber-crime and explain two ways cyber-crime can negatively affect a business. (6 marks)

b) Discuss four major technological factors that you would consider when procuring a data-loss preventer tool. (8 marks)

c) Define the term Active Directory hence evaluate its function in managing any file servers. (6 marks)

QUESTION THREE (20 MARKS)

a) Define the following information system terminologies as captured in the Kenya data Protection ACT.
   i. Data Processor
   ii. Data subject
   iii. Data Controller. (6 marks)

b) Illustrate ways in which control objectives for Informational and related Technology (COBIT) assists in managing system security associated risk. (8 marks)

c) Discuss three specific function of a firewall in securing a computer Network. (6 marks)

QUESTION FOUR (20 MARKS)

a) As an I.T manager in your organisation, list four ways you can plan and ensure ICT resource security is maintained at an acceptable level. (8 marks)

b) Using a diagram, briefly explain the TCP-3-WAY Handshake. (8 marks)

c) Differentiate between 2FA and MFA (4 marks)