MURANG'A UNIVERSITY OF TECHNOLOGY

SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY

UNIVERSITY POSTGRADUATE EXAMINATION

2024/2025 ACADEMIC YEAR

FIRST YEAR FIRST **SEMESTER** ONE EXAMINATION FOR

DOCTOR OF PHILOSOPHY IN INFORMATION TECHNOLOGY

SIT 901-INFORMATION SECURITY AND GOVERNANCE

DURATION: 3 HOURS

INSTRUCTIONS TO CANDIDATES:

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

QUESTION ONE (25 MARKS)

A company experienced a data breach after failing to update its threat model with recent intelligence on emerging phishing attacks, leaving it vulnerable to a sophisticated phishing campaign.

a) Explain how real time threat intelligence be incorporated into threat modelling to improve the accuracy and relevance of identified risk. (10 marks)

b) Describe how you would tailor a threat modelling technique to meet the specific security requirements of a high-risk industry (e.g. healthcare or finance), considering regulatory constraints and unique threat landscape. Provide examples to support your approach.

(15marks)

QUESTION TWO (25 MARKS)

a) Provide a brief definition of information security management system (ISMS) and point out three benefits of ISMS to any organization. (9 marks)

b) Giving relevant examples differentiate between each of the following information security domains:

   (a) Administrative (2 marks)

   (b) Physical (2 marks)

   (c) Technical (2 marks)

c) Cloud computing is becoming popular as many enterprise application and data are moving into cloud adoption is real and perceived lack of security. Cloud security must grow and evolve to face these threats and provide a bulwark defence for consumers that leverage the effectiveness and advantages cloud services is in the cloud. Discuss the cyber security issues in the cloud that businesses have to deal with today and in the future. (10 marks)

QUESTION THREE (25 MARKS)

a) Andrew and Sons Corp has decided to share threat information among sharing partners. Garry a threat analyst, working in Andrews and Sons Corp has asked to follow a trust model necessary to establish trust between sharing partners. In the trust model used by him the first organization makes use of a body of evidence in the second organization, and the level of trust between two organization depend on the degree and quality of evidence provided by the first organization discuss how the validation trust model applied to the above case.

(10 marks)

b) Describe the defence in depth model of technology security and how it works. (15 marks)

QUESTION FOUR (25 MARKS)

a) Most networked systems are adopting cryptographic to secure information and data.
   i. With examples explain how cryptography ensure data confidentiality and integrity in networked environments. (8 marks)
   ii. Discuss the trade-off between public and secret key cryptography in practical application. (7 marks)

b) Evaluate the security challenges associated with managing cryptographic keys in distributed systems and how the concept of public key infrastructure (PKI) address the complexities of key generation, distribution, revocation and archiving. (10 marks)

QUESTION FIVE (25 MARKS)

a) Compare and contrast signature based and anomaly based detection methods in terms of their effectiveness and limitations. (10 marks)

b) Discuss the importance of secure programming principles specifically–input validation, least privilege and secure coding practices in mitigating common vulnerabilities with software systems. In your response, provide an in depth analysis of how the absence of these principles can lead to security breaches. (15 marks)