MURANG'A UNIVERSITY OF TECHNOLOGY

SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY

TVET EXAMINATION

2023/2024 ACADEMIC YEAR

SECOND YEAR **SECOND** SEMESTER EXAMINATION FOR DIPLOMA IN INFORMATION TECHNOLOGY

IT-OS-ICT-CR-03-6-A - CONTROL ICT SECURITY THREAT

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) Define the term computer security.   (2 marks)
b) List any three physical threats to a computer system.   (3 marks)
c) Explain any three ways attackers may use to identify on individual password. (6 marks)
d) Outline four important functions that information security performs for an organization.
                                                                         (4 marks)
e) Giving an example, explain the term cyber security threat.   (4 marks)
f) Describe identity theft as used in computer security.   (4 marks)
g) Highlight four symptoms of a computer virus.   (4 marks)
h) State three ways that you can use to prevent Brute Force attack.   (3 marks)

SECTION B – ANSWER ANY TWO QUESTIONS IN THIS SECTION

QUESTION TWO (20 MARKS)

a) Discuss five elements of an information security policy.   (10 marks)
b) Discuss the following types of malicious ware.   (10 marks)
      i.   Viruses
     ii.   Trojans
    iii.   Worms
    iv.   Ransomware
     v.   Spyware

QUESTION THREE (20 MARKS)

a) State any five types of computer security testing.   (5 marks)
b) Outline any seven ways one can use to prevent identify theft.   (7 marks)
c) Discuss any four cyber security risks in the banking industry and suggest how each can be minimised.   (8 marks)

QUESTION FOUR (20 MARKS)

a) Explain each of the following terms as used in computer security.   (10 marks)
      i.   Firewall
     ii.   Hacking
    iii.   Threat
    iv.   Vulnerability
     v.   Risk
b) Explain three main objectives of information security.   (6 marks)
c) Give four rules that must be observed in order to keep within the law when working with data information.   (4 marks)

QUESTION FIVE (20 MARKS)

a) Discuss any six (6) measures you can advise an organization to apply to protect itself from cyber-attacks.   (12 marks)
b) Outline four ways of preventing piracy with regard to data and information.   (4 marks)
c) Distinguish between data security and data integrity as used in ICT security. (4 marks)