**061006T4ICT**

**ICT Technician Level 6**

**ICT/OS/IT/CR/3/6**

**CONTROL ICT SECURITY THREATS**

**Mar. /Apr. 2023**

**Time: 3 Hours**

****

**THE KENYA NATIONAL EXAMINATIONS COUNCIL**

**WRITTEN ASSESSMENT**

**3 Hours**

**INSTRUCTIONS TO CANDIDATES**

***Maximum marks for each question are indicated in brackets ( ).***

***This paper consists of TWO sections: A and B.***

***Answer questions as per instructions in each section.***

***You are provided with a separate answer booklet*.**

***The candidates should answer the questions in English***

Section A (40 marks)

*Answer ALL the questions in this section*

1. Define the term computer security. (2 Marks)
2. List any **three** physical threats to a computer system. (3 Marks)
3. State **three** ways that you can use to prevent Brute Force attacks. (3 Marks)
4. State any **three** ways attackers may use to identify an individual password. (3 Marks)
5. List **three** ways data from within the organization may be exposed or accessed by unauthorized entity. (3 Marks)
6. Explain each of the following terms as used in computer security. (10 Marks)
7. Firewall
8. Hacking
9. Threat
10. Vulnerability
11. Risk
12. Explain **three** classifications of computer hackers. (6 Marks)
13. Outline **four** important functions that information security performs for an organization.

(4 Marks)

1. Outline **two** reasons why it is important to use a VPN when accessing internet using a public network. (2 Marks)
2. Differentiate between Vulnerability Assessment and Penetration Testing. (4 Marks)

**Section B (60 marks)**

*Answer* ***any THREE*** *questions in this section*

1. a) Cyber security poses a major threat to many organizations. Explain **five** essentials cyber security measures a business firm should consider. (10 Marks)

b) A rise in hybrid working has made businesses more vulnerable than ever to cybercrime**.** Discuss any **five** common threats to an organization. (10 Marks)

1. a) Define identity Theft as used in computer security. (3 Marks)

b) Outline any **seven** ways one can use to prevent identity theft. (7 Marks)

c) Discuss the following types of malicious ware. (10 Marks)

1. Viruses
2. Trojans
3. Worms
4. Ransomware
5. Spyware
6. a) Explain **five** ways of preventing man-In-The-Middle (MITM) attack. (10 Marks)

b) Discuss steps for establishing an Secure Sockets Layer (SSL) connection. (10 Marks) (10 Marks) (20 Marks)

1. a) Different types of security testing offer a reliable means for organizations to strengthen the cyber security posture. State any **six** types of computer Security Testing. (6 Marks)

b) Information security is a key factor in an organization. Explain **three** main objectives of Information security. (6 Marks)

c) Discuss **four** elements of an Information Security Policy. (8 Marks)

**THIS IS THE LAST PRINTED PAGE**