061006T4ICT

ICT TECHNICIAN LEVEL 6

IT/OS/ICT/CR/3/6

CONTROL ICT SECURITY THREATS

JULY/ AUGUST 2023

TVET CURRICULUM DEVELOPMENT, ASSESSMENT AND CERTIFICATION COUNCIL (TVET CDACC)

WRITTEN ASSESSMENT

TIME: 3 HOURS

INSTRUCTIONS TO CANDIDATE

1. This paper has two sections **A and B.** Attempt questions in each section as per instructions given in the section.
2. You are provided with a separate answer booklet.
3. Marks for each question are indicated in the brackets.
4. Do not write on the question paper

This paper consists of THREE (3) printed pages

Candidates should check the question paper to ascertain that all pages are printed as indicated and that no questions are missing

SECTION A: (40 MARKS)

Attempt ALL questions in this section.

1. Using an example of appropriate techniques in each case, discuss THREE goals of ICT security. (6 Marks)
2. State the security concept that has the ability to prove that a sender sent an encrypted message. (1 Mark)
3. Mary copies files from her desktop computer to a USB flash device and puts the device into her pocket. Explain a security concern that may arise. (2 Marks)
4. Outline the reason why a layered security is a good practice in building secure ICT environments. (2 Marks)
5. Discuss THREE common categories of ICT security threats. (6 Marks)
6. Identify THREE reasons of physical security in protecting ICT systems. (3 Marks)
7. Describe the following DoS attacks;
    a) Ping flood (2 Marks)
    b) SYN Flood (2 Marks)
    c) HTTP/HTTPS Flood (2 Marks)
8. Penetration testing is essential to identifying vulnerabilities in organization's systems and networks. Identify FOUR ethical penetration-testing techniques. (4 Marks)
9. ICT security policies define how an organization deals with security aspects. Using an example in each case, differentiate between user policies and system administration policies. (4 Marks)
10. Describe the following ICT Security controls giving an example for each. (6 Marks)
    a) Preventive Controls
    b) Detective Controls
    c) Corrective Controls
    d) Deterrent Controls

SECTION B: (60 MARKS)

Attempt any THREE (3) questions in this section.

11. Bethany Nursing Home, a large hospital in Kenya, is concerned about the security of its ICT systems and the potential risks to patient data.
    a) As an ethical hacker preparing a detailed vulnerability management plan for the hospital, discuss FIVE tasks that will be necessary to carry out. (10 Marks)
    b) The hospital's management is concerned about the legal implications of computer crimes that could threaten its ICT systems, programs and data. To assure the management of legal safety in case of a crime, clearly explain FIVE types of crimes covered by the Kenya Computer Misuse and Cybercrimes Act, 2021. (10 Marks)
12. A leading banking institution in Uganda is planning to enhance its physical security measures to protect its branches and critical ICT infrastructure from unauthorized access and potential threats. As a security consultant discuss;
    a) FIVE physical security measures that the bank could implement. (10 Marks)
    b) FIVE data security measures that the bank could implement. (10 Marks)

13. The Ministry of Tourism, Wildlife & Heritage (GoK) - Head Office has recently experienced a series of ICT security incidents, including unauthorized access to sensitive data and disruptions in critical systems. As an ICT security officer in the ministry,
    a) Explain FIVE potential ICT security threats that the ministry may be facing and the threats' effects. (10 Marks)
    b) Recommend TWO appropriate measures to mitigate each of the identified threats. (10 Marks)
14. Fast Movers Lt d, a logistics company has recently had its data vulnerable to unauthorised access by its employees and outside hackers. In once serious instance, the network was breached and a massive volume of data was stolen and not fully recovered. A key concern has been poor device management where employees log in to organisational systems using their personal computers and mobile phones. In addition, the company procures its IT hardware from just any vendor who meets a low-price requirement.
    a) To address the highlighted weaknesses and others that may be present, recommend five ways to improve the company's ICT policies. (10 Marks)
    b) ii) Identify five potential challenges of implementing ICT security measures. (10 Marks)