**061206T4CYB**

**CYBER SECURITY TECHNICIAN LEVEL 6**

**SEC/OS/CS/CR/11/6/A**

**MANAGE SECURITY OPERATIONS**

**Nov. / Dec. 2023**

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

## CANDIDATE'S WRITTEN ASSESSMENT

**Time: 3 hours**

## INSTRUCTIONS TO CANDIDATES

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

**This paper consists of 3 printed pages.**

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

## SECTION A: (40 MARKS)

*Answer **all** questions in this section*

**1.** Define the following terms as used in management of security operations. (***2 marks***)

a) Asset

b) Inventory

**2.** Jitume Computer Software Ltd wants to develop an information assets inventory. Highlight SIX steps the company will follow to achieve this objective. (**6 *marks***)

**3.** Describe THREE assets that may be classified according to an organization's Inventory Management Policy. (***6 marks***)

**4.** Setting up an assets inventory in an organization is of paramount importance. Explain THREE advantages that can be achieved by setting up an assets inventory in an organization.

(***6 marks***)

**5.** List THREE factors to consider in the acquisition of a security management system in an organization. (***3 marks***)

**6.** System misconfigurations are a major cause of security breaches. As a cybersecurity technician outline FOUR breaches that could occur due to misconfigurations of systems.

(***4 marks***)

**7.** Identify THREE strategies that can be employed in hardening of a security management system. (3 ***marks***)

**8.** Explain TWO settings that can be performed when configuring a dashboard of a security management system. (4 ***marks***)

**9.** Highlight any THREE types of threats you are likely to encounter in management of a system security. (***3 marks***)

**10.** As a cyber-security consultant, you have been tasked by Tarakilishi Computer Services Ltd. to institute measures that can mitigate against system security threats for their company. State THREE measures in managing system threats. (***3 marks***)

## SECTION B: (60 MARKS)

***Answer question ELEVEN (11) and any other TWO questions***

**11**. You are a cybersecurity analyst working for Vibrant Cyber Security Company that specializes in developing cutting-edge software solutions. Your organization has recently experienced a significant increase in cyber threats, ranging from sophisticated malware attacks to targeted phishing campaigns. The management team has recognized the need to establish a comprehensive threats landscape to enhance the company's cybersecurity posture.

Based on the above narrative develop a threats landscape for Vibrant Cyber Security Company. ***(20 marks)***

**12**.a) Kipeperushi Computers and Accessories Ltd. are in the process of acquiring a Security Information and Event Management (SIEM) Software, following your advice as the lead system security consultant. Explain to them any FIVE benefits of such a system. **(*10 marks*)**

b) Jack is a senior tutor at Maendeleo Vocational Training Institute and was training I.C.T technicians Level 6 on generating a security operations report. Discuss any FIVE components of a security operations report. **(*10 marks*)**

**13.a)** Tujilinde Computer Services Ltd company recently formed a Computer Incident Response Team (CIRT) to help the company in situation of system security breaches. Discuss FIVE roles that such a team would be mandated to perform. **(*10 marks*)**

**b)** Cyber security is a rapidly evolving field, and keeping abreast with emerging trends is crucial to staying ahead of cyber threats. Discuss FIVE emerging trends in cyber security. **(10 *marks*)**

**14.a)** Akiba Bank Ltd Information Technology Manager noticed a brutal force attack attempt on the bank’s financial system. Explain FIVE techniques that the manager could institute to prevent future attacks happening. **(*10 Marks*)**

**b)** Mary an IT technician was conducting a continuous monitoring of the system noticed that some data was missing from the system. Describe FIVE events that could have caused data loss in the organization. **(*10 marks*)**