**JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS**

**UNIVERSITY EXAMINATION FOR THE DEGREE OF COMPUTER SECURITY & FORENSICS / BUSINESS INFORMATION SYSTEMS**

**1st YEAR 1st SEMESTER 2024/ 2025 ACADEMIC YEAR**

---

**COURSE CODE: ICB1101**

**COURSE TITLE: PC SECURITY AND PRIVACY**

**EXAM VENUE: MAIN CAMPUS**

**DATE: STREAM: CSF/BIS**

**TIME: 2 HOURS EXAM SESSION:**

---

**INSTRUCTIONS:**

1. **Answer question 1 in Section A (Compulsory) and any other two questions in Section B**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

**QUESTION ONE (30 MARKS)**

a) Define the following terms as used in PC security and Privacy (6 marks)

i) Risk

ii) Vulnerability

iii) Threat

b) OSI model concept was designed to standardize the system of communication between devices in a network, it consists of seven layers. Name and explain the OSI layers in networking. (10 marks)

(c) Describe how a man-in-the-middle (MITM) attack works and provide an example of how it can be mitigated. (3 marks)

d). You are tasked with securing a company's workstations against ransomware attacks. What measures would you take to minimize the risk? (5 marks)

e). How can organizations foster a culture of security awareness among employees? What policies or training programs would you implement? (3 marks)

f). Explain the difference between symmetric and asymmetric key encryption. (3 marks)

**QUESTION TWO (20 MARKS)**

a). You receive an email from your bank telling you there is a problem with your account. The email provides instructions and a link so you can log in to your account and fix the problem. As a student taking PC security and privacy unit, state FOUR things that you can do (4 marks)

b). State the principle of the least privilege. Why is it important? (3 marks)

c) Briefly explain the critical function of a firewall in IT network (4 marks)

d). Explain your role as a user in protecting your personal computer (3 marks)

e). Weak Passwords are always one of the vulnerabilities most frequently targeted by someone trying to break into a system. Discuss? (3 marks)

f). State THREE primary functions of a firewall in PC security? (3 marks)

**QUESTION THREE (20 MARKS)**

a). State five biometric security controls and explain how they work. (5 marks)

b). Briefly explain THREE disadvantages of Symmetric key cryptography (3 marks)

c). Discuss at least five active threats to a computerized system in an organizations (5 marks)

d). Explain TWO differences between active and passive attack giving examples in each case. (2 marks)

e). State the five elements of an internal control process (5 marks)

**QUESTION FOUR (20 MARKS)**

a). Outline FOUR safety precautions and practices that computer users observe while in computer laboratory (4 marks)

b). Explain how access control lists are used to represent access control matrices and their **TWO** advantages and disadvantages. (6 marks)

c) Explain what is meant by a digital signature and describe how it is generated (5 marks)

d). Employees are increasingly connecting to company networks remotely via mobile devices such as laptops, tablets and smart-phones. Remote access needs to satisfy five essential requirements to be efficient and secure. Identify and briefly explain each of these FIVE requirements (5 marks)

**QUESTION FIVE (20 MARKS)**

a). State and Explain Computer security best practices that would be suitable for small to medium size business (5 marks)

b). Define the following terms as used in Information system control objectives (4 marks)

i. Crypto Systems

ii. Public key infrastructure

c). State **FOUR** consequences of ignoring computer security to an organization (4 marks)

d). Briefly explain Defense in Depth and how the strategy is implemented in computer security (5 marks)

e). State two differences between a worm and a virus (2 marks)

***This is the last printed page***