JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF COMPUTER SECURITY AND FORENSIC WITH IT

1st YEAR 1st SEMESTER 2022/ 2023 ACADEMIC YEAR

COURSE CODE: **ICB 1101**

COURSE TITLE: **PC SECURITY AND PRIVACY**

EXAM VENUE: **MAIN CAMPUS**

DATE: **STREAM: COMPUTER SECURITY AND FORENSIC**

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 (6Mks)

i) Economy of mechanism

ii) Least priviledge

iii) Least common mechanism

b) Security policy is considered to be a living document which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes. State **FOUR** reasons why organization need security policies. (8Mks)

(c) The mouse on your computer screen starts to move around on its own and click on things on your desktop. As a student taking a unit in PC security and privacy, state THREE ways on what you can do. (3Mks)

d).What is the difference between the Internet and the World Wide Web. Create at least three statements that identify the differences between the two. (5Mks)

e). State and explain the FOUR essential steps of the Risk Management Process (5Mks)

f). Explain the THREE ways in which identity theft can be prevented (3Mks)

QUESTION TWO (20MARKS)

a). An organization makes each lead system administrator responsible for the security of the system he or she runs. However, the management determines what programs are to be on the system and how they are to be configured.

i. Describe the security problem(s) that this division of power would create. (4Mks)

ii). How would you fix the problem (3Mks)

b) Briefly explain the critical function of a firewall in IT network (4Mks)

c). Explain your role as a user in protecting your personal computer (3Mks)

d). Weak Passwords are one of the vulnerabilities most frequently targeted by someone trying to break into a system. Discuss (4Mks)

e). What is phishing and how is it a security threat (2Mks)

QUESTION THREE (20MARKS)

a). Briefly explain THREE disadvantages of Symmetric key cryptography (3Mks)

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

c). Computer security is both fascinating and complex. State and explain any Five challenges to Computer Security (5Mks)

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

e). State five biometric security controls and explain how they work. (5Mks)

QUESTION FOUR (20Marks)

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

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

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

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 (5Mks)

QUESTION FIVE (20Marks)

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

b). Biometric technology has been available for a number of years; however its adoption has been slow. Discuss FOUR factors that inhibits or delay the adoption of biometric technologies. (4Mks)

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

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

e). A while back, the IT people got a number of complaints that one of our campus computers was sending out Viagra spam. They checked it out, and the reports were true: a hacker had installed a program on the computer that made it automatically send out tons of spam email without the computer owner's knowledge.

i. How do you think the hacker got into the computer to set this up? (2Mks)