JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF INFORMATION AND COMMUNICATION TECHNOLOGY

2ND YEAR 2ND SEMESTER 2024/2025 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ITB 1210

COURSE TITLE: IT SECURITY

EXAM VENUE: STREAM: BSC. INFORMATION AND COMMUNICATION TECHNOLOGY

DATE: 16/4/2025
EXAM SESSION: 15.00- 17.00
VENUE: CL 1
TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two questions**
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 1 (30 marks)

a) What **TWO** roles does anomaly detection play in network monitoring? 2mks

b) State TWO reasons why it is important to regularly update software and systems? 2mks

c) How can organizations protect data at rest and in transit? 2mks

d) Explain what an access control list (ACL) is and how it functions. 2mks

e) Explain the concept of a Virtual Private Network (VPN) and TWO of its benefits. 3mks

f) What are some of the **TWO** best practices for managing mobile devices as part of endpoint security? 2mks

g) State and Explain **TWO** different types of data backups? 2mks

h) Explain **TWO** ways how you can prevent SQL Injection attacks? 2mks

i) Explain the potential risks of misconfiguring security settings in each cloud service model (IaaS, PaaS, SaaS)? 3mks

j) What are the risks of neglecting the shared responsibility model? 2mks

k) What is pretexting, and how is it used in social engineering attacks? Provide ONE example.

3mks

l) Identify ONE team member who should be included in the incident response team, and state ONE of their respective roles? 2mks

m) What is ISO 27001? 1mk

n) What is the NIST Cybersecurity Framework? 2mks

Question 2 (20 marks)

a) Your IT organization is required by the regulators to prepare a compliance audit report. You have been chosen to be part of the team responsible for this, identify and describe TEN issues you will need to consider when preparing for a compliance audit (e.g., ISO 27001, PCI DSS)?

10mks

b) What is the purpose of post-incident analysis (PIA)? Explain EIGHT information that should be included in a PIA report? 10mks

Question 3 (20 marks)

a) Describe the concept “human Firewall”. Explain EIGHT steps an organization can take to strengthen the "human firewall" and reduce the risk of social engineering attacks? 10mks

b) State and explain FIVE key practices you can employ to implement a DevSecOps approach in the cloud? 5mks

c) What is Data Loss Prevention (DLP)? Explain FOUR ways how DLP systems work. 5mks

Question 4 (20 marks)

a) State and explain **FIVE** common types of threats to endpoint security? 5mks
b) Explain the **THREE** main types of access control models, and how do they differ? 6mks
c) Describe what an IT security policy is? Explain the **FOUR** main components of an IT security policy? 9mks

Question 5 (20 marks)

a) Identify and Describe **FIVE** common tools used for network monitoring and analysis? 10mks

b) Explain the **FIVE** core functions of the NIST Cybersecurity Framework. How can organizations use the framework to improve their cybersecurity posture? 10mks