Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES

BACHELOR OF SCIENCE IN COMPUTER NETWORKS AND CYBER SECURITY
END OF SEMESTER EXAMINATION
CNS 2103: INTRODUCTION TO CYBER SECURITY

DATE: 24th July 2023 Time: 2 Hours

Instructions

1. This examination consists of **FIVE** questions.
2. Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

QUESTION ONE [30 MARKS]

a) (i) Explain the importance of cyber security fundamentals in protecting information systems. (5 Marks)

(ii) Describe three different types of malware and their characteristics. (6 Marks)

b) Explain the concept of digital identity and its significance in ensuring online security. (4 Marks)

c) Discuss the role of access management in maintaining information security. (5 Marks)

d) Define cyber security threats and breaches, and discuss their potential impact on organizations. (5 Marks)

e) Explain the concept of ethical hacking and its role in ensuring system security. (5 Marks)

QUESTION TWO [20 MARKS]

a) Describe three different types of cyber-attacks and their objectives. (6 Marks)

b) Explain three prevention strategies that organizations can implement to protect against cyber-attacks. (6 Marks)

c) Discuss the importance of basic cryptography in ensuring data confidentiality. (8 Marks)

QUESTION THREE [20 MARKS]

a) Explain the concept of preventive software and its role in protecting against malware and other cyber threats. (6 Marks)

b) Discuss the significance of a security policy in establishing a secure computing environment. (6 Marks)

c) Describe the key elements of an incidence response plan and their importance in handling security incidents. (8 Marks)

QUESTION FOUR [20 MARKS]

a) Discuss the concept of business information continuity and its role in maintaining operational resilience. (5 Marks)

b) Explain the process of incident response and its importance in mitigating the impact of security incidents. (6 Marks)

c) Discuss three common types of security breaches and the measures organizations can take to prevent them. (9 Marks)

QUESTION FIVE [20 MARKS]

a) Explain the concept of access management and its significance in controlling user permissions and privileges. (6 Marks)

b) Discuss the role of security awareness training in promoting a culture of cybersecurity within organizations. (6 Marks)

c) Describe the principles of secure software development and their importance in building resilient applications. (8 Marks)