OFFICE OF THE DEPUTY VICE CHANCELLOR
ACADEMICS, STUDENT AFFAIRS AND RESEARCH

UNIVERSITY EXAMINATIONS

2023/2024 ACADEMIC YEAR

THIRD YEAR SECOND SEMESTER EXAMINATION

FOR THE DEGREE OF BACHELOR OF COMPUTER SCIENCE

MAIN EXAM

COURSE CODE: **COM 323**

COURSE TITLE: **INFORMATION SYSTEMS SECURITY**

DATE: 16-APRIL-24 **TIME:** 9:00AM - 12:00PM

INSTRUCTION TO CANDIDATES

- **SEE INSIDE**

THIS PAPER CONSISTS OF PRINTED PAGES **PLEASE TURN OVER**

MAIN EXAM
COM 323: INFORMATION SYSTEMS SECURITY
STREAM: BSc (Computer Science) **DURATION: 3 Hours**

INSTRUCTIONS TO CANDIDATES

i. *Answer **ALL** questions from section A and any **THREE** from section B.*

ii. *Maps and diagrams should be used whenever they serve to illustrate the answer.*

iii. *Do not write on the question paper.*

SECTION A (24 MARKS) COMPULSORY

QUESTION ONE [12 MARKS]

a) Describe the primary role of each of the following entities in information security management.

i. Information Owner **[1 Marks]**

ii. Information Custodian **[1 Marks]**

iii. Information User **[1 Marks]**

b) Differentiate between ***Authentication*** and ***Authorization*** and highlight the role of each in information systems security. **[4 Marks]**

c) Describe with the aid of a suitable diagram, the relationship between the following terms as relates to information systems security; *"**vulnerability**", "**threat**", "**attack**", "**breach impact**" and "**control**".* **[5 Marks]**

QUESTION TWO [12 MARKS]

a) Enumerate on the role of ***personnel training*** in enhancing Information Systems Security, citing two relevant real-life examples. **[2 Marks]**

b) Information System Security is said to be both a "***management issue***" and "***People Issue***". With reference to roles played by these two communities, defend this statement. **[2 Marks]**

c) Discuss the concept of *public key encryption infrastructure* and its application in information security for information systems that extend to the internet. **[2 Marks]**

d) At any point in time, Data/Information in the information systems of an enterprise exists in three states: in *storage*, on *transit* or being *processed*. For each state, identify one security *vulnerability*, *threat*, possible *type of attack* and suggested security *counter measure*.

[6 Marks]

SECTION B {36 MARKS}

QUESTION THREE [12 MARKS]

a) Using an example of a large insurance company, discuss **THREE** possible triggers of information systems security policy document reviews. **[3 Marks]**

b) Recommend a strategy for assessing the level of ***adherence*** and ***compliance*** with security policies in an organization. **[4 Marks]**

c) Analyze how the approach used in the implementation of security in information systems could lead to poor state of the system security. **[2 Marks]**

d) Explain any **THREE** roles of information Systems Security audits. **[3 Marks]**

QUESTION FOUR [12 MARKS]

a) Discuss the roles of human resources department in the *implementation* and *enforcement* of security policies. **[3 Marks]**

b) Information Systems Security policy is a core pillar in the security of information. Recommend the best possible strategy for *developing*, *implementing* and *enforcing* information security policies in an organization. **[5 Marks]**

c) Discuss the concept of *monitoring* as used in Information Systems Security and highlight any **FOUR** reasons that may compel an administrator to implement Information Systems monitoring. **[4 Marks]**

QUESTION FIVE [12 MARKS]

a) Evaluate how the *personnel* component in information systems may be a threat to information security. **[3 Marks]**

b) Identify the **THREE** core elements of *security risk management* in information systems and describe **TWO** activities under each element. **[6 Marks]**

c) Explain the key components of an effective plan for enterprise data backup. **[3 Marks]**

QUESTION SIX [12 MARKS]

a) Recommend a strategy for implementing enterprise information system security **[3 Marks]**

b) Describe the *McCumber Cube Security Model* and how it guides in the effective implementation of information systems security. **[6 Marks]**

QUESTION SEVEN [12 MARKS]

a) Enumerate on the role of information systems security in an enterprise. **[2 Marks]**

b) Describe with the aid of a diagram and clear examples, the relationship between the following items: Policies, Standards, Guidelines, Practices and procedures. **[6 Marks]**

c) Describe each of the following Access Control Methods; *Rule Based Access*, *Role Based Access*, *Discretionary Access Control* and *Mandatory Access Control*. **[4 Marks]**

END OF EXAM