(Knowledge for Development)

KIBABII UNIVERSITY

(KIBU)

UNIVERSITY EXAMINATIONS
2021/2022 ACADEMIC YEAR

END OF SEMESTER EXAMINATIONS
YEAR THREE SEMESTER TWO EXAMINATIONS

FOR THE DEGREE IN
(COMPUTER SCIENCE)

COURSE CODE : CSC 321

COURSE TITLE : COMPUTER SYSTEM SECURTY

DATE: 31/8/2022 **TIME:** 9.00 A.M - 11.00 A.M

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTIONS ONE AND ANY OTHER TWO.

QUESTIONS ONE (COMPULSORY) [30 MARKS]

a) Define the following terms **[5 marks]**

i) System

ii) Security

iii) System security

iv) Information security

v) Information assurance

b) Identify and discuss the fundamental goals of system security **[8 marks]**

c) A computer can be either or both the subject of an attack and/or the object of an attack, explain the statement **[5 marks]**

d) State and explain the components of information security **[6 marks]**

e) Explain the three causes of information security **[6 marks]**

QUESTION TWO [20 MARKS]

a) Identify five threat categories and in each category, give a relevant example **[10 marks]**

b) Differentiate between a hacker and a cracker **[4 marks]**

c) State and explain any three types of attack to information systems **[6 marks]**

QUESTION THREE [20 MARKS]

a) What is authentication **[2 marks]**

b) Describe three authentication methods **[9 marks]**

c) Discuss three forms of access control **[9 marks]**

QUESTION FOUR [20 MARKS]

a) State and explain five forms of physical security **[10 marks]**

b) Discus how an intrusion detections system and different from a firewall **[10 marks]**

QUESTION FIVE [20 MARKS]

Hillary Clinton was accused of keeping classified information on her private email server she used during her tenure as a secretary of state.

a. As a security professional, briefly describe the steps you will take to prevent occurrence of such information security lapses. **[6 marks]**

b. The USA government discovered the Hillary Clinton was using her private email server after she had left the position of secretary of state. Briefly suggest the best course of action you would take to prevent any possible attack as a result of the incident giving your reasons for the chosen course of action **[3 marks]**

c. Discuss the security risks posed by her action with respect to information assurance core principles. **[4 marks]**

d. Discuss the techniques used by antivirus in detecting virus in a computer system **[7 marks]**