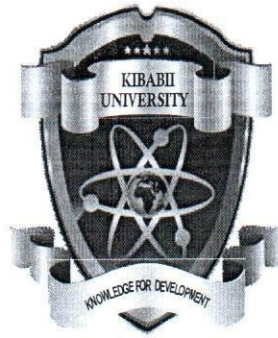# KIBABII UNIVERSITY (KIBU)

MAIN CAMPUS

UNIVERSITY EXAMINATIONS

END OF SEMESTER EXAMINATION

2021/2022 ACADEMIC YEAR

THIRD YEAR FIRST SEMESTER EXAMINATION

FOR THE DEGREE OF BACHELORS OF SCIENCE IN

(INFORMATION TECHNOLOGY & COMPUTER SCIENCE)

COURSE CODE: BIT 313

COURSE TITLE: INFORMATION ASSURANCE AND SECURITY

DATE: 19/05/2022   **TIME:** 9.00 A.M. – 11.00 A.M.   **2HRS**

INSTRUCTIONS TO CANDIDATES:
ANSWER QUESTION ONE AND ANY OTHER TWO.

QUESTION ONE (COMPULSORY) [30 MARKS]

a. Define Information assurance and security. **[2 marks]**

b. Discuss the difference between information assurance and information security. **[4 marks]**

c. Information assurance should be viewed as spanning four security engineering domains; state and explain the four engineering domains. **[4 marks]**

d. Information assurance, focuses on ensuring the availability, integrity, authentication, confidentiality, and non-repudiation of information and systems, give the difference between integrity and non-repudiation. **[2 marks]**

e. Traditionally, computer facilities have been physically protected for three reasons, give the three reasons. **[3 marks]**

f. Name and explain at least three Cyber Crime Prevention Tips. **[3 marks]**

g. An Issue-specific policy is concerned with a certain functional aspect that may require more attention. For this reason, a separate policy is prepared for that issue to explain with details the required level of security, and the instructions that all staff in the organization must abide by to achieve this level. Give at least FOUR examples for this type of policy. **[4 marks]**

h. Define Policy as used in information security policies, standards and practices. **[2 marks]**

i. Information assurance is based on three principles explain these principles. **[3 marks]**

j. The offensive players in the world of Information Warfare come in six types, discuss at least three. **[3 marks]**

QUESTION TWO [20 MARKS]

a. Differentiate between Hacker and Criminal as used in information assurance and security. **[2 marks]**

b. The security policy is a high-level document that defines the organization's vision concerning security, goals, needs, scope, and responsibilities. List the three main types of policies. **[3 marks]**

c. The flip side of Information Assurance is Information Warfare. Explain the three types of information warfare. **[6 marks]**

d. Discuss the three Information assurance levels stating the Desired Effects. Attacker's Operations and Defender's Operations on each. **[9 marks]**

QUESTION THREE [20 MARKS]

a. Explain at least two benefits of information assurance. **[2 marks]**

b. Discuss at least **SIX** Threats to Information Security. **[6 marks]**

c. As an information assurance and security expert state and explain The Six Data Protection Principles. **[12 marks]**

QUESTION FOUR [20 MARKS]

a. IT Security Policy and Guidelines provides references and guidance to Government bureau and departments in respect of the protection of information systems and data assets. Explain the following IT security policy and guidelines

   i. Baseline IT Security Policy **[2 marks]**

   ii. IT Security Guidelines **[2 marks]**

   iii. Practice Guide for Security Risk Assessment & Audit **[2 marks]**

   iv. Practice Guide for Information Security Incident Handling. **[2 marks]**

b. State and explain the three Critical Skills for Cyber Security Professionals. **[6 marks]**

c. Explain the difference between Computer intrusions and Data privacy as used in information assurance and security. **[4 marks]**

d. Authorization is determining what a subject can access after authentication state the two types of authorization. **[2 marks]**

QUESTION FIVE [20 MARKS]

a. Discuss the five most pressing ethical and legal issues confronting the industry today in information assurance and security. **[10 marks]**

b. Information system is the entire set of components necessary to use information as a resource in the organization, discuss the six components of an information system. **[10 marks]**