



(Knowledge for Development)

**KIBABII UNIVERSITY
(KIBU)**

**UNIVERSITY EXAMINATIONS
2022/2023 ACADEMIC YEAR**

**END OF SEMESTER EXAMINATIONS
THIRD YEAR FIRST SEMESTER**

**FOR THE DEGREE IN
(INFORMATION TECHNOLOGY)**

COURSE CODE: BIT 313

**COURSE TITLE: INFORMATION ASSURANCE
AND SECURITY**

DATE: 20/12/2022 TIME: 2.00 P.M - 4.00 P.M

INSTRUCTIONS

ANSWER QUESTIONS ONE AND ANY OTHER TWO.

QUESTION ONE (COMPULSORY) [30 MARKS]

- a. Define Information assurance and security. **[2 Marks]**
- b. 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]**
- c. Information assurance should be viewed as spanning four security engineering domains. Explain. **[4 Marks]**
- d. State the difference between Information assurance and information security. **[2 Marks]**
- e. Illustrate the three information assurance levels. **[3 Marks]**
- f. What is the difference between Network Security and Internet Security? **[2 Marks]**
- g. Define Botnet as used in information assurance and security. **[2 Marks]**
- h. Give at least two benefits of information security. **[2 Marks]**
- i. Define Computer security as used in Information assurance and security. **[2 Marks]**
- j. Traditionally, computer facilities have been physically protected for three reasons: Explain. **[3 marks]**
- k. Vulnerability is the intersection of three elements: discuss the three elements. **[3 marks]**
- l. What is Vulnerability management? **[3 marks]**

QUESTION TWO [20 MARKS]

- a. Explain the three principles that Information assurance is based on. **[3 Marks]**
- b. With the aid of well labeled diagrams explain the difference between Passive attack and Active attack. **[6 Marks]**
- c. 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. Illustrate the following terms as used in IT Security Policy and Guidelines **[4 Marks]**
 - i. Baseline IT Security Policy
 - ii. IT Security Guidelines
 - iii. Practice Guide for Security Risk Assessment & Audit

- iv. Practice Guide for Information Security Incident Handling
- d. Policy Management defines three types of security policy: explain the three types of security policy. **[3 marks]**
- e. Standards define the obligatory rules, instructions, and/or actions required to realize the goals and objectives set by the top management in the security policies. Discuss **[3 marks]**
 - i. Baseline
 - ii. Guidelines
 - iii. Procedures
- f. Define security policy as used in information assurance and security **[1 mark]**

QUESTION THREE [20 MARKS]

- a. The flip side of Information Assurance is Information Warfare (IW). In fact, one can think of the offensive part of IW as "information operations," and the defensive part as information assurance. Discuss the three types of Information Warfare. **[6 Marks]**
- b. With the aid of well labeled diagrams illustrate what is meant by interruption, modification interception, fabrication siting examples on each. **[8 Marks]**
- c. Discuss the Six Data Protection Principles. **[6 Marks]**

QUESTION FOUR [20 MARKS]

- a. The offensive players in the world of Information Warfare (IW) come in six types, Illustrate at least three. **[6 Marks]**
- b. Explain Peer entity authentication. **[2 marks]**
- c. Discuss the following Threats to Information Security. **[4 marks]**
 - i. Phishing
 - ii. SQL Injection
- d. What the difference between Bottom-Up Approach and Top-Down Approach as used in Information Security Implementation. **[4 marks]**
- e. State the three main types of policies. **[3 marks]**
- f. Define Policy as used in information assurance and security. **[1 marks]**

QUESTION FIVE [20 MARKS]

- a. State the difference between Backdoors and Zombie computers. **[2 marks]**
- b. State and explain at least three Cyber Crime Prevention Tips. **[6 marks]**
- c. Differentiate between Connection-Oriented Integrity Service and Connectionless-Oriented Integrity Service. **[4 marks]**
- d. Explain the Three Critical Skills for Cyber Security Professionals. **[3 marks]**
- e. As information technology becomes increasingly influential, the ethical and legal considerations become similarly relevant. Explain the five most pressing ethical and legal issues confronting the industry today. **[5 marks]**