KAIMOSI FRIENDS UNIVERSITY

THIRD YEAR SECOND SEMESTER UNIVERSITY EXAMINATIONS
2025/2026 ACADEMIC YEAR

SPECIAL EXAMINATIONS

FOR THE DEGREE OF BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

COURSE TITLE: INFORMATION ASSURANCE AND SECURITY II

COURSE CODE: BIT 323

DATE: 22/6/2026 **TIME: 12-2PM**

INSTRUCTIONS TO STUDENTS

1. Answer **QUESTION ONE** and **ANY OTHER TWO** from the choices given.
2. Phones, smart watches, ear phones or any other unauthorized digital and AI gadgets and applications are **NOT ALLOWED IN** the examination room.
3. Answer all questions in the exam answer booklet provided.
4. Do not write on this question paper.
5. All KAFU examination rules and regulations apply.
6. DURATION OF EXAMINATION: **TWO (2) HOURS**

KAFU observes ZERO tolerance to examination cheating.

QUESTION ONE (30 MARKS) – COMPULSORY

i. Define the following terms as used in information system security [6 Marks]
   - Economy of mechanism
   - Least privilege
   - Least common mechanism

ii. Explain three ways in which identity theft can be prevented. [3 Marks]

iii. Differentiate between active attack and passive attack [2 Marks]

iv. Briefly explain Defense in Depth and how the strategy is implemented in information security. [5 Marks]

v. Prevention must be taken in the collection, preservation, and examination of electronic evidence. Explain how electronic evidence is handled at crime scene. [7 Marks]

vi. Explain any three evidences of computer intrusion. [3 Marks]

vii. Explain the role of expert in court of law. [4 Marks]

QUESTION TWO

i. List any three attributes of a good information system auditor [3 Marks]

ii. Explain how you can apply the scientific methods in digital investigations. [4 Marks]

iii. After securing the scene of crime what would you do if the computer monitor is found to be off in order to avoid losing data. [8 Marks]

iv. Outline any two electronic devices from which we can collect electronic evidence. [2 Marks]

v. Explain what is the risk based audit. [3 Marks]

QUESTION THREE

a) Briefly explain three disadvantages of symmetric key cryptography. [3 Marks]

b) Discuss how you would secure and evaluate a crime scene in preparation for forensic investigations [10 Marks]

c) Based on ISO 27001:2013 standard outline the basic attributes of the security policy should have. [7 Marks]

QUESTION FOUR

i. Using a well-labeled diagram, describe the stages of risk assessment process. [14 Marks]

ii. Explain how you would conduct a closing audit meeting. [6 Marks]

QUESTION FIVE

a) You have been contracted to carry out an ISMS audit in Kenya Power Company. Provide an audit plan that can be used during the exercise. [6 Marks]

b) Explain the code of conduct for professional that you know off. [6 Marks]

c) With the aid of three examples and based on the ISO 27001:2013 explain the statement of applicability. [6 Marks]

d) Mention any two ways a computer can be used in executing crime. [2 Marks]