



## **UNIVERSITY EXAMINATIONS**

### **EXAMINATION FOR SEPTEMBER/DECEMBER 2025/2026 DIPLOMA IN CYBER SECURITY | DIPLOMA IN ETHICAL HACKING AND INFORMATION SECURITY**

#### **DICS 6113: INTRODUCTION TO INFORMATION SECURITY**

DATE: 2<sup>nd</sup> December, 2025

TIME: 2 HOURS

#### **GENERAL INSTRUCTIONS:**

Students are NOT permitted to write on the examination question paper during exam time.

This is a closed book examination. Text book/Reference books/notes are not permitted.

#### **SPECIAL INSTRUCTIONS:**

This examination paper consists Questions in Section A followed by section B. Answer Question 1 and any Other Two questions.

QUESTIONS in ALL Sections should be answered in answer booklet(s).

- 1. PLEASE start the answer to EACH question on a NEW PAGE.**
- 2. Keep your phone(s) switched off at the front of the examination room.**
- 3. Keep ALL bags and caps at the front of the examination room and DO NOT refer to ANY unauthorized material during the course of the examination.**
- 4. ALWAYS show your working.**
- 5. Marks indicated in parenthesis i.e. ( ) will be awarded for clear and logical answers.**
- 6. Write your REGISTRATION No. clearly on the answer booklet(s).**
- 7. For the Questions, write the number of the question on the answer booklet cover page in the order you answered them.**
- 8. DO NOT use your PHONE as a CALCULATOR.**
- 9. YOU are ONLY ALLOWED to leave the exam room 1hour to the end of the Exam.**
- 10. DO NOT write on the QUESTION PAPER. Use the back of your BOOKLET for any calculations or rough work.**

## SECTION A (COMPULSORY)

### QUESTION 1 (30 Marks)

**a.** Define the following terms and explain their relevance in Information Security: **(10 marks)**

- i.** Cybercrime
- ii.** Data Protection
- iii.** Digital Forensics
- iv.** Ethics
- v.** Security Policy

**b.** The Computer Misuse and Cybercrimes Act (2018) and the Data Protection Act (2019) form the backbone of Kenya's cybersecurity legal framework.

- i.** Discuss **five (5)** major provisions from these two laws and explain how each provision helps organizations enhance cybersecurity. **(10 marks)**

**c.** A company discovers that an employee has been secretly collecting customers' phone numbers and selling them to a third-party marketing firm. Using **ethical principles** and **policy guidelines**, analyze the situation and recommend actions the organization should take. **(10 Marks)**

Your answer must include:

- i.** Ethical issues involved
- ii.** Relevant policy violations
- iii.** Possible legal consequences
- iv.** Correct organizational response

## SECTION B (ANSWER ANY TWO QUESTIONS)

### QUESTION 2 (20 Marks)

- a.** Explain the CIA triad with suitable examples. **(8 Marks)**
- b.** Analyze one trade-off organisations face in balancing confidentiality, integrity and availability. **(6 Marks)**
- c.** Propose practical measures to balance CIA in an SME. **(6 Marks)**

### QUESTION 3 (20 Marks)

- a.** Identify four (4) essential components of an information security program. **(7 Marks)**
- b)** Discuss how risk management integrates with these components. **(6 Marks)**
- c)** Design a simple roadmap for implementing a security program in a small enterprise. **(7 marks)**

### QUESTION 4 (20 Marks)

- a.** Define incident response and describe its main phases. **(8 Marks)**
- b.** Analyze the importance of containment, eradication, and recovery in limiting damage. **(6 Marks)**

- c. Evaluate the role of post-incident review in improving organisational resilience. **(6 Marks)**

**QUESTION 5 (20 Marks)**

- a. List and briefly explain two legal or regulatory frameworks relevant to information security. **(6 Marks)**
- b. Examine ethical considerations in handling personal data. **(7 Marks)**
- c. Propose strategies organisations can use to balance operational needs with compliance. **(7 Marks)**