



UNIVERSITY EXAMINATIONS

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

DICS 6112: DATA SECURITY

DATE: 11th 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 as used in the context of data security:
(10 Marks)
- i.** Tokenization
 - ii.** Insider Threat
 - iii.** Zero Trust Architecture
 - iv.** Data Minimization
 - v.** Security Policy
- b.** Explain five (5) common causes of data breaches in modern organisations.
(5 Marks)
- c.** State and briefly explain five (5) data protection principles drawn from GDPR/Data Protection.
(5 Marks)
- d.** Distinguish between symmetric and asymmetric encryption with suitable examples and give one real-world use case for each.
(4 Marks)
- e.** Describe three (3) methods organisations use to ensure data availability.
(6 Marks)

SECTION B (ANSWER ANY TWO QUESTIONS)

QUESTION 2 (20 Marks)

- a.** Explain the concept of access control in securing data.
(5 Marks)
- b.** Illustrate with examples how RBAC differs from DAC in protecting data.
(8 Marks)
- c.** Evaluate the effectiveness of these models in preventing insider threats.
(7 Marks)

QUESTION 3 (20 Marks)

- a.** Define encryption, hashing, and digital signatures, giving one use case each.
(6 Marks)
- b.** Demonstrate how cryptographic tools enforce confidentiality, integrity, and authenticity.
(7 Marks)
- c.** Critically assess the limitations of relying solely on cryptography for data security.
(7 marks)

QUESTION 4 (20 Marks)

- a.** Define data classification and outline four classification levels with examples.
(7 Marks)
- b.** Analyze how classification influences handling, storage, and disposal of data.
(6 Marks)
- c.** Propose a classification policy for a healthcare organisation managing patient data
(7 Marks)

QUESTION 5 (20 Marks)

- a.** Identify three risks of storing sensitive data in the cloud. **(6 Marks)**
 - i. Examine how encryption and key management address these risks. **(7 Marks)**
 - ii. Recommend additional technical and contractual measures an organisation should take. **(7 Marks)**