UNIVERSITY EXAMINATIONS

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

DICS 6222: DESKTOP SERVER SECURITY

DATE: 9th 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 desktop & server security (**10 Marks)**

- **i.** Server hardening
- **ii.** Patch management
- **iii.** Endpoint protection (EPP / EDR)
- **iv.** Active Directory (AD)
- **v.** Principle of Least Privilege (PoLP)

b. Explain five (5) common causes of desktop and server security incidents/breaches in organisations. **(5 Marks)**

c. State and briefly explain five (5) best-practice principles for securing servers. **(5 Marks)**

d. Distinguish between patch management and configuration management with suitable examples. **(4 Marks)**

e. Describe three (3) methods organisations use to ensure availability of desktop and server resources. **(6 Marks)**

SECTION B (ANSWER ANY TWO QUESTIONS)

QUESTION 2 (20 Marks)

a. Define access control and explain its importance in desktop and server security. **(5 Marks)**

b. Compare and contrast any two access control models with examples. **(7 Marks)**

c. Recommend the most suitable model for a financial institution, justifying your choice. **(8 Marks)**

QUESTION 3 (20 Marks)

a. List and briefly explain four (4) items in a pre-deployment server security checklist. **(6 Marks)**

b. Demonstrate how patching and system hardening reduce vulnerabilities before deployment. **(8 Marks)**

c. Assess the importance of conducting a baseline audit before going live. **(6 marks)**

QUESTION 4 (20 Marks)

a. Differentiate between antivirus and endpoint detection & response (EDR). **(6 Marks)**

b. Explain how EDR improves incident detection and response compared to antivirus**.** **(7 Marks)**

c. Propose a migration strategy for an organisation moving from antivirus to EDR. **(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)**