



End Term (Even) Semester Examination June 2025

Roll no.....

Name of the Course and semester: MTech II
Name of the Paper: Applied Cyber Security(S)
Paper Code: MCS - 232

Time: 3 hour

Maximum Marks: 100

Note:

- (i) All the questions are compulsory.
- (ii) Answer any two sub questions from a, b and c in each main question.
- (iii) Total marks for each question is 20 (twenty).
- (iv) Each sub-question carries 10 marks.

Q1.	(2X10=20 Marks)	CO1
a.	Define malware and describe its major types. Illustrate with examples how each type can affect a computer system.	
b.	Explain the concept of social engineering. How can organizations educate employees to defend against it?	
c.	Design a multi-layered defense mechanism to prevent phishing, spoofing, and spam-based attacks in an enterprise.	
Q2.	(2X10=20 Marks)	CO2
a.	Compare copyright, patent, and software licensing. Recommend suitable protections for a software product developed by a startup.	
b.	Define information security governance. Explain its components and design a basic structure for a mid-sized IT company.	
c.	What is ISO 27001? Explain its importance in information security and outline the steps to begin ISO implementation in a small firm.	
Q3.	(2X10=20 Marks)	CO3
a.	Analyze a recent public breach where Wi-Fi security protocols failed, and suggest a remediation strategy using WPA3 and WIPS.	
b.	Propose a secure remote access architecture for a globally distributed workforce using VPNs and MFA.	
c.	What is a firewall? Explain its types with examples and suggest an appropriate firewall setup for a college campus.	
Q4.	(2X10=20 Marks)	CO4
a.	Evaluate different database auditing techniques and recommend an optimal model for high-frequency financial transactions.	
b.	Analyze the ethical and legal implications of penetration testing without formal consent in enterprise environments	
c.	Define penetration testing. Outline its steps and apply it to a scenario involving a vulnerable university database.	
Q5.	(2X10=20 Marks)	CO5
a.	What is disaster recovery planning? Identify its phases and apply it to a real-world cyberattack scenario.	
b.	Explain types of backups. Recommend a backup strategy for a healthcare provider.	
c.	Explain the structure of an ISO 27001 compliance report. Draft a simple outline that a small business might use.	