ICLED BUSINESS SCHOOL

SUMMER SEMESTER, 2025

Postgraduate Diploma in Cybersecurity and Artificial Intelligence

Answer any 5 questions. Each Question Carries 20 marks

Question 1:

a) Explain the CIA triad (Confidentiality, Integrity, Availability) and its significance in security design.
b) Differentiate between prevention, detection, and recovery as security goals, providing examples for each.

Question 2:

a) Analyze the role of trust and assumptions in enforcing security policies and mechanisms.
b) Discuss how human factors and organizational issues impact cybersecurity implementation.

Question 3

a) Compare traditional intrusion detection systems with AI-driven IDS, highlighting benefits and limitations.
b) Explain anomaly detection using machine learning and its application in cybersecurity.

Question 4

a) Discuss the role of AI in automated incident response and SOAR platform integration.
b) Identify key challenges of implementing AI in cybersecurity.

Question 5:

a) Define adversarial machine learning and explain how adversarial examples compromise AI models

b) Discuss model poisoning and data tampering risks in AI pipelines.

Question 6

a) Explain privacy-preserving techniques in AI systems.
b) Evaluate best practices for secure AI development.

Question 7

a) Differentiate between security policies and mechanisms, providing examples of each.
b) Discuss the composition problem in policy design and its implications for security.

Question 8

a) Define Advanced Persistent Threats (APT) and explain why they pose significant risks.
b) Discuss adversarial attacks on AI systems and their implications for critical infrastructure.