VIT
Vellore Institute of Technology

REG.NO.:

SCHOOL OF COMPUTER SCIENCE ENGINEERING AND INFORMATION SYSTEMS
CONTINUOUS ASSESSMENT TEST-I
FALLSEMESTER 2025-2026

SLOT: D1+TD1

Programme Name & Branch : B.Tech(IT)
Course Code and Course Name : BITE413L-Cyber Security
Faculty Name(s) : Dr. SRINIVAS KOPPU, Dr.RAMYA.G
Class Number(s) : VL2025260105237, 5236
Date of Examination : 20-8-2025
Exam Duration : 90 minutes **Maximum Marks: 50**

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)
- Course Outcomes
  CO1-Analyze the importance of cybersecurity and cybercrime.
  CO2-Recommend the importance of mobile and wireless device security

Q. No	Question	M	CO	BL
1.	Discuss in detail the classification of cybercrimes by method of attack, providing at least one real-world case study for each category.	10	CO1	BL1
2.	Classify the different types of IP rights applicable in the digital environment, including copyright, patents, trademarks, and trade secrets. For each category, describe its purpose, scope of protection, and examples of cyber-related violations, along with preventive measures.	10	CO1	BL1
3.	A multinational energy company's CEO receives a phone call from someone claiming to be a senior government official requesting urgent documents for a "national security audit." The caller uses insider jargon and threatens legal consequences if the CEO delays. Within 2 hours, sensitive blueprints are emailed to an unverified address. Analyze the psychological manipulation techniques used here and map them to the social engineering kill chain. Propose a multi-step verification protocol for high-value requests that can be implemented without frustrating executives.	10	CO1	BL2
4.	A 12-year-old plays an online multiplayer mobile game. An attacker posing as another child befriends them in chat, gradually extracting personal details and convincing them to share private photos via another app. Map the grooming process from initial contact to exploitation. Recommend both in-game moderation controls and parental monitoring strategies to detect early signs of grooming.	10	CO2	BL2
5.	Discuss how organizations can prevent and detect SIM swapping attacks through mobile security policies and employee guidelines.	10	CO2	BL2

****