

Register No.: Name:

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

FIFTH SEMESTER INTEGRATED MCA DEGREE EXAMINATION (R), DECEMBER 2023 (2020 SCHEME)

Course Code: 20IMCAT307

Course Name: Fundamentals of Information Systems Security

Max. Marks: 60

Duration: 3 Hours

PART A

(Answer all questions. Each question carries 3 marks)

1. Using a neat sketch, explain the three components of the CIA triangle.
2. Why is the top down approach to information security superior to the bottom up approach?
3. Identify any five threats to information security. Give an example for each.
4. What measures can individuals take to protect against shoulder surfing?
5. What does it mean by risk likelihood? What is its objective?
6. Which are the different data classification schemes available? Which scheme is used by the military?
7. What is sacrificial host? What is bastion host?
8. What is a circuit gateway? How does it differ from the other forms of firewalls?
9. Which are the three methods of data interception? Explain each.
10. With a suitable diagram, explain digital forensics process.

PART B

(Answer one full question from each module, each question carries 6 marks)

MODULE I

11. Define an information system. Describe the various components and critical characteristics of it. (6)

OR

12. Using a block diagram, explain the different phases of implementing information systems security in an organization. (6)

MODULE II

13. Explain the following attacks. (6)
 - i) Denial-of-Service (DoS)
 - ii) Social engineering
 - iii) Malicious code

OR

14. Define intellectual property. Which are the different types of IP? How does IP help an organization to create more value for itself? (6)

MODULE III

15. Discuss the process of identifying risks and vulnerabilities in an organization with a suitable diagram. (6)

OR

16. Describe the "mitigate" risk control strategy. List and describe the three common plans. (6)

MODULE IV

17. How do screened host architectures for firewalls differ from screened subnet firewall architectures? Which of these offer more security for the information assets that remain on the trusted network? (6)

OR

18. Discuss the various protocols available for securing communications and transactions in the web and internet. (6)

MODULE V

19. List and describe the four basic conversion strategies that are used when converting to a new system. Under which circumstances is each of these the best approach. (6)

OR

20. Describe the role of security management maintenance model in maintaining systems. (6)
