Register No.: .... Name: ....

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

FIFTH SEMESTER INTEGRATED MCA DEGREE EXAMINATION (S), FEBRUARY 2024
(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. Explain the three core characteristics of information that are essential for understanding its value in information security. How do these characteristics impact the goals of information security?
2. List and briefly describe the primary goals of information security. How do these goals help organizations in achieving a secure and resilient information environment?
3. Explain the importance of protecting the functionality of information systems to meet the business needs of an organization.
4. Explain the difference between a threat and an attack in the context of information security. Provide a real-world example of each to illustrate your explanation.
5. How does trust impact an organization's ability to manage and mitigate security and privacy risks? Provide an example to illustrate this relationship.
6. Explain the key challenges associated with securing mobile and portable systems.
7. Discuss the role of access control, password security and firewalls in enhancing information security.
8. Explain the significance of protecting remote connections and the role of intrusion detection and prevention systems in achieving this goal.
9. How do physical access controls help prevent unauthorized interception of data? What are some key elements in the implementation and maintenance of effective physical security measures?
10. How does effective project management contribute to the success of information security projects? What are some key considerations in this process?

PART B

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

MODULE I

11. a) Describe the key implementation issues that organizations may encounter while striving to achieve the goals of information security. Provide specific examples or scenarios to illustrate these issues. (3)

b) Explain the concept of security in the systems life cycle, emphasizing its importance in the development and maintenance of secure information systems. (3)

OR

12. a) Explain the key components of the need for security in information systems. Provide examples of how each component is essential for ensuring information security. (3)

b) Discuss the challenge of balancing security and access in information systems. How can organizations strike a balance between stringent security measures and the need for legitimate users to access information and resources effectively? Provide practical strategies or examples. (3)

MODULE II

13. a) Explain what malicious code is and how it can be used in cyberattacks. Provide examples of different types of malicious code and the potential risks they pose to information security. (3)

b) Discuss the concept of "back doors" in the context of information security with a real-world example. How are back doors created? What are the implications for organizations if they are exploited by malicious actors? (3)

OR

14. a) Define the terms "Denial of Service" and "Distributed Denial of Service." Explain the key differences between these attacks and provide examples of how they can impact organizations' IT systems. (3)

b) Discuss strategies and countermeasures that organizations can employ to mitigate the impact of Denial of Service and Distributed Denial of Service attacks. Provide examples of preventive and responsive measures that can help protect against these types of attacks. (3)

MODULE III

15. a) Discuss the challenges individuals and organizations face in protecting personal computers in today's information technology landscape. Explain how these challenges have evolved with advancements in technology and changes in the threat landscape. (3)

b) Describe common types of attacks that personal computers can be vulnerable to. Explain how security measures and practices can be employed to mitigate the risks associated with these attacks and protect personal computers effectively. (3)

OR

16. a) Explain the process of risk identification in the context of information security. How can organizations effectively identify potential risks and vulnerabilities in their information systems? Why is this an essential first step in the risk management process? (4)

b) Discuss the importance of risk assessment and risk control in managing information security risks. Explain the key steps and methods involved in risk assessment. Describe the strategies organizations can use to control or mitigate identified risks. (2)

MODULE IV

17. a) Explain the concept and significance of digital signatures in the context of secure communication and authentication. How do digital signatures work ? (4)

b) Discuss the role and importance of digital certificates in the field of information security. (2)

OR

18. a) Explain the concept and significance of Public Key Infrastructure (PKI) in the field of information security. How does PKI work? What role does it play in providing secure communication, authentication and data integrity in the digital realm? (3)

b) Discuss the key components and processes involved in a typical PKI system. Explain the roles of entities such as Certificate Authorities (CAs), registration authorities, and end-users. (3)

MODULE V

19. a) Explain the concepts of Information Systems Security Certification and Accreditation (C&A). How do these processes ensure that information systems meet security standards and are authorized for use in an organization? (3)

b) Discuss the importance of Information Systems Security C&A in the context of compliance, risk management and overall information security governance. (3)

OR

20. a) Explain the concept of Security Management Maintenance Models, highlighting their importance in maintaining an effective security posture. Describe some common models and their key principles for ensuring ongoing security in organizations. (3)

b) Discuss the role of digital forensics in investigating cybercrimes and security incidents. Explain the steps involved in a typical digital forensics investigation. Describe the tools and techniques used to collect, preserve, and analyze digital evidence. (3)

****