DECEMBER 2022 **P/ID 16311/PIT3J**

Time : Three hours Maximum : 80 marks

PART A — (10 × 2 = 20 marks)

Answer any TEN questions.

1. What are the types of security attacks?

2. What are the characteristics of Information Security?

3. Define coupling and cohesion.

4. What is operating system security and protection?

5. Define address protection in operating system.

6. Define Reliability and Integrity.

7. State the relationship between security and precision.

8. What is single point of failure?

9. Define public key infrastructure.

10. What is business continuity plan?

11. How is information to be protected legally?

12. What is copyright infringement?

PART B — (5 × 6 = 30 marks)

Answer any FIVE questions.

13. Discuss the various types of threats to information.

14. What is the difference between attack and vulnerability? List and explain any seven attacks.

15. Briefly explain the basic security requirement of database systems.

16. Discuss the problems in defining the boundaries of the network with suitable diagram.

17. With an example discuss the concept of social engineering attack.

18. Explain the seven issues that are addressed in the security plan.

19. Discuss the four levels in which the organisation has classified all its data resources.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

20. Describe in detail the controls for preserving confidentiality, integrity and availability.

21. Discuss the protection objects and security methods in operating system.

22. Explain the issues or problems that are associated with the biometrics. State the difference between identification and authentication.

23. Define IDS and discuss the components of intrusion detection system with suitable diagram.

24. Describe why computer crime is hard to define and to prosecute.
