DECEMBER 2022 **P/ID 40553/PCI1C**

Time : Three hours Maximum : 80 marks

PART A — (10 × 2 = 20 marks)

Answer any TEN questions in 50 words each.

1. Theft of information

2. Vulnerability in Information Security

3. Malicious Code

4. Secret in Information classification

5. Confidential in Information classification

6. Cost analysis

7. User Identity

8. Risk Mitigation

9. Fire Detection

10. Access Management

11. Physical Assets

12. Threat Identification

PART B — (5 × 6 = 30 marks)

Answer any FIVE questions in 250 words each.

13. Information Security is challenged by cybercrime criminal- Do you agree?

14. Why should we classify information?

15. How to determine Probability of Occurrence?

16. Define Access and Privilege Management.

17. How to identify assets to be protected?

18. Elucidate about Business Requirements.

19. Explain about Account Authorization.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions in 500 words each.

20. Explain Security Policies. Use an illustration to explain.

21. Explain Information Classification and De-classification.

22. Explain the impact of threat on information.

23. Elucidate on Cryptography. Give a detail note on Encryption and Decryption.

24. Explain Perimeter Security. Give its importance (at least 12)