DECEMBER 2020 **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. Cyber frauds.

2. Information.

3. DDOS.

4. Need for security policy.

5. Custodian Authorization for Access to information.

6. Why should information be disposed safely?

7. Cyber Threats.

8. Authorized Access to information.

9. Event Logging.

10. Cryptography.

11. Physical Security.

12. Fire Prevention.

PART B — (5 × 6 = 30 marks)

Answer any FIVE questions in 250 words each.

13. What is Social Engineering? How it is used to commit Frauds?

14. Explain Tier three security policy.

15. Declassification of information- Discuss.

16. Elucidate Risk Analysis Process.

17. Elucidate on Threat Identification.

18. How will you monitor system access control?

19. Write a note on Perimeter Security.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions in 500 words each.

20. Write a detail note on information security procedures to be adopted in a company.

21. Explain the authorization of information access for different users.

22. Write a detail note on Cost analysis.

23. Discuss in detail the IDS in access control.

24. Write a note on identification of assets to be protected.