Note: Answer all questions from Part A. Answer any five questions from Part B.

PART – A (25 Marks)

1. State the critical characteristics of information. 3
2. Define network security. 2
3. Differentiate policy and law. 3
4. What is the difference between vulnerability and exposure? 2
5. What is firewall? 2
6. List the applications of content filters. 3
7. What is cryptography and cryptanalysis? 3
8. Give any four names of substitution techniques. 2
9. What is digital forensics, and when is it used in a business setting? 3
10. List and describe the three major steps in executing the project plan. 2

PART – B (50 Marks)

11. List and define the factors that are likely to shift in an organization’s information security environment. 10

12. What is Intrusion Detection System (IDS)? What are different types of Intrusion Detection Systems available? Explain with diagrams. 10

13. Explain in detail:
   i) Firewalls categorized by processing mode 5
   ii) Different generations of firewall 5

14. Explain in detail different risk control strategies. 10

15. Explain in detail the Security System Development Life Cycle (Sec SDLC). 10

16. Explain with examples various threats to Information Security. 10

17. Write short notes on:
   i) Incident Response Plan (IRP) 5
   ii) Strength of DES. 5