(For candidates admitted from 2016–2017 onwards)

U.G. DEGREE EXAMINATION, NOVEMBER 2022.

Part IV — Information Technology – Non-Major Elective

INFORMATION SECURITY : PRINCIPLES AND PRACTICES

Time : Three hours Maximum : 75 marks

PART A — ($10 \times 2 = 20$)

Answer ALL questions.

1. What is Information Security?
2. Define vulnerability.
3. List out some examples of issue-specific policy.
4. What is Ring of trust?
5. Define Evaluation Assurance Level.
6. List out the category of Computer Crimes.
7. Mention the physical Security threats for Information Security.

8. What is configuration and change management?

9. Define Authentication.

10. What is cryptography?

PART B — (5 × 5 = 25)

Answer ALL questions, choosing either (a) or (b).

11. (a) List out the task of the Information Security Specialist.

Or

(b) Write notes on Risk management.

12. (a) What are the types of Security Policies?

Or

(b) Elaborate on Trust Computing Base.

13. (a) Write notes on Protection Profile Organization.

Or

(b) Write short notes on Computer Forensics.

14. (a) Explain the Physical Security Domain.

Or

(b) What are the interdependencies exits in computer security controls?

15. (a) Write short notes on Mandatory and Role based Access Control.

Or

(b) What is the role of keys in cryptography?

PART C — (3 × 10 = 30)

Answer any THREE questions.

16. Discuss about the umbrella of Information Security.

17. Explain the suggested standards taxonomy for security.

18. Explain about the Intellectual Property Law.

19. Elaborate on the Operations Security Controls in Action.

20. Discuss about biometrics and its role in enhancing security.

———————