Register Number:……

**B.TECH., DEGREE EXAMINATIONS NOV/DEC 2012**

Seventh & Fifth Semester

**INFORMATION TECHNOLOGY**

ITY122: Information Security

**Time: Three Hours** **Maximum Marks:100**

**Answer ALL Questions:-**

**PART A (10x1=10 Marks)**

1. Which of the following will not protect you from spam?

   A) spam blockers B) e-mail rules C) popup blocker D) filters

2. If configured correctly, the _____ will prevent interaction with your computer after a specified time period.

   A) firewall B) filter C) screen saver D) popup blocker

3. A program that migrates through networks and operating systems by attaching itself to different programs and databases is a

   A) Virus B) Worms C) Damage D) Denial-of-service

4. CBA

   A) Committee on Business Application B) Common Business Application

   C) Commercial Business Application D) Cost Benefit Analysis

5. ---------- is the expected percentage of loss that would occur from a particular attack.

   A) Single Loss Expectancy B) Exposure Factor

   C) Double Loss Expectancy D) Policy developer's

6. In which one of the following documents is the assignment of individual roles and responsibilities MOST appropriately defined?

   A) Security policy B) Enforcement guidelines

   C) Acceptable use policy D) Program manual

7. Which of the following embodies all the detailed actions that personnel are required to follow?

   A) Standards B) Guidelines C) Procedures D) Baselines

8. What is the MAIN purpose of a change control/management system?

   A) Notify all interested parties of the completion of the change.

   B) Ensure that the change meets user specifications.

   C) Document the change for audit and management review.

   D) Ensure the orderly processing of a change request.

9. A 'Psuedo flaw' is which of the following?

A) An apparent loophole deliberately implanted in an operating system program as a trap for intruders

B) An omission when generating Psuedo-code

C) Used for testing for bounds violations in application programming

D) A normally generated page fault causing the system to halt

10. Access control techniques do not include which of the following choices?

A) Relevant Access Controls B) Discretionary Access Controls

C) Mandatory Access Controls D) Lattice Based Access Controls

**PART B (10 x 2 = 20 Marks)**

11. What decision is taken based on the feasibility study during logical design?
12. What does a hacktivist do?
13. What is the difference between vulnerability and exposure?
14. What are the three components of the C.I.A. triangle? Why is it incompetent?
15. What is meant by base lining?
16. Define a policy.
17. Define security blueprint.
18. What does a proxy server do?
19. Why is a contingency plan prepared?
20. Who is a tailgater? How to overcome this threat?

**PART C (5 x 14 = 70 Marks)**

21. a) (i) List the categories of threat. Explain each one of them with suitable examples.

**(OR)**

b) (i) What are the critical characteristics of Information. (4)

(ii) Write short notes on the components of Information security. (10)

22. a) (i) List the major types of attacks. (4)

(ii) Explain the various types of attacks. (10)

**(OR)**

b) Explain in detail the Legal, Ethical and Professional Issues in Information Security.

23. a) Write short notes on:

(i) Risk Appetite (2)

(ii) Delphi Technique (2)

(iii)Benchmarking (3)

(iv) Explain how an appropriate risk control strategy is selected. (7)

**(OR)**

b) Explain how risk assessment is done.

24. a) Write short notes on:

(i) Issue-specific security policy (8)

(ii) System-specific security policy (6)

**(OR)**

b) Give the major process steps in ISO 17799 / BS7799 and explain them.

25. a) (i) Why IDS is necessary? (4)

(ii) Explain the network-based and host-based IDS. (10)

**(OR)**

b) Explain in detail the physical access controls.

**********