National Institute of Technology, Delhi

Name of the Examination: B.Tech./M.Tech/MCA/Ph.D.

Mid Semester Examination (Spring, Feb-2026)

Branch : B. Tech. CSE
Semester : VI
Title of the Course : Information Security
Course Code : CSBB 335
Time: 1.5 Hour
Maximum Marks: 25

Note: All questions are compulsory.

COURSE OUTCOMES		COGNITIVE LEVELS
CO1	Understand information security fundamentals including CIA triad, terminology, roles, and responsibilities.	L2
CO2	Analyze threats, vulnerabilities, risks and recommend suitable mitigation strategies.	L4
CO3	Demonstrate information security policies, standards, procedures, and governance mechanisms.	L3
CO4	Analyze security technologies, assessment procedures, and evaluation methods for systems and networks.	L4
CO5	Analyze and apply basic cryptographic techniques and access control mechanisms in practical scenarios.	L4

Attempt all questions from each section.

Section-A (1x 5 = 5 Marks)
(MCQ/Fill in the blanks/one line /one-word questions/statements etc.)

Qs. No.	Question	CO	BL	PO
1.	The Information Technology department is the owner of which information asset? A) Personnel data B) All security devices C) Only servers and desktops D) All technological assets except data	CO1	L2	PO1
2.	The process of access control involves: A) Identification B) Authentication C) Authorization D) Access	CO3	L3	PO1, PO2
3.	A company stores sensitive data but does not patch its operating systems regularly. Which risk is most likely to increase? A) Natural disaster risk B) Exploitation of known vulnerabilities C) Data redundancy D) Improved compliance	CO2	L4	PO2, PO3
4	Consider the following statements regarding Operational Controls: 1. They deal with the operational functionality of security in the organization. 2. They include personnel security, physical security, and protection of production inputs and outputs. 3. They primarily focus on high-level strategic planning and policy formulation. 4. They mainly address tactical and technical design issues of security systems. Which of the above statements are correct? A) 1 and 2 only B) 1, 2 and 3 only C) 2 and 4 only D) 1, 2, 3 and 4	CO1	L2	PO1, PO2
5	Policy management documents must be managed and nurtured as they are constantly changing and growing. For them to remain viable, they must have: A) Proper documentation and protected passwords B) Encrypted passwords C) An indication of effective and revision date or schedule of reviews	CO3	L3	PO1, PO11

	D) All of the above			

Section-B (2.5 x 4 = 10 Marks) (Short Questions)				
Qs. No.	**Question**	**CO**	**BL**	**PO**
6.	Describe management groups that are responsible for implementing information security to protect the organization's ability to function?	CO3	L3	PO1, PO2
7.	List the various types of malware? Compare worms from viruses? Explain "Trojan horses carry viruses or worms"?	CO2	L4	PO1, PO3
8.	Explain that data is the most important asset an organization possesses. Also explain what other assets in the organization require protection.	CO1	L2	PO1
9.	Define risk management? Analyze the importance of identifying risks by listing organizational assets and their vulnerabilities in the risk management process.	CO2	L4	PO1, PO2

Section-C (5 x 2 = 10 Marks) (Long Questions)				
Qs. No.	**Question**	**CO**	**BL**	**PO**
10.	a. Compare Administrative Controls and Technical Controls with examples. b. Explain the effect of Denial-of-Service attacks on availability. List out type of controls that can prevent such attacks?	CO3	L3	PO1, PO2
11.	a. Explain the CIA Triad (Confidentiality, Integrity, Availability) as the foundation of information security? b. Discuss threats to each goal and explain how appropriate controls help to maintain CIA.	CO1	L2	PO1, PO2