.

Printed Page:-3 **Subject Code:- AMTCY0216**

Roll. No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute Affiliated to AKTU, Lucknow)
M.Tech
SEM: II - THEORY EXAMINATION (2025 - 2026)
Subject: Information Security

Time: 3 Hours **Max. Marks: 70**

General Instructions:

IMP: *Verify that you have received the question paper with the correct course, code, branch etc.*

1. *This Question paper comprises of* ***three Sections -A, B, & C.*** *It consists of Multiple Choice Questions (MCQ's) & Subjective type questions.*

2. *Maximum marks for each question are indicated on right -hand side of each question.*

3. *Illustrate your answers with neat sketches wherever necessary.*

4. *Assume suitable data if necessary.*

5. *Preferably, write the answers in sequential order.*

6. *No sheet should be left blank. Any written material after a blank sheet will not be evaluated/checked.*

SECTION-A 15

1. Attempt all parts:-

(1.1) Tick the maximum duration of protection granted by a utility patent. (CO1,K1) 1

(a) 10 years
(b) 15 years
(c) 20 years
(d) 25 years

(1.2) Select the correct purpose of served by policy review within an organization. (CO2,K2) 1

(a) To create new policies
(b) To evaluate the effectiveness of existing policies
(c) To enforce policy compliance
(d) To communicate policies to employees

(1.3) Implementing face recognition for attendance monitoring helps in. (CO3,K1) 1

(a) Email filtering
(b) User productivity tracking
(c) Eliminating proxy attendance
(d) Enhancing network speed

(1.4) Select a risk mitigation method suitable for remote access environments. (CO4,K1) 1

(a) Font Smoothing
(b) Browser Tabbing
(c) VPN Implementation
(d) USB Formatting

.

(1.5) Recognize the component of ISO 700 focused on risk assessment. (CO5,K1) 1

(a) Annex A
(b) Schedule B
(c) Chapter C
(d) Title D

2. Attempt all parts:-

(2.1) Describe the need of information security. (CO1,K1) 2

(2.2) Explain electronic payment system and its benefits. (CO2,K2) 2

(2.3) Show how physical security prevents unauthorized entry. (CO3,K3) 2

(2.4) Recognize basic principles of application development security. (CO4,K2) 2

(2.5) Explain the relationship between IT Act provisions and digital transactions. (CO5,K2) 2

SECTION-B 20

Answer any one of the following:-

(3.1) List the best practices for secure data backup and recovery. (CO1,K2) 4

(3.2) Describe the role of antivirus software in information security. (CO1,K1) 4

Answer any one of the following:-

(3.3) Explain backup. Define its type. (CO2,K1) 4

(3.4) Define Backup security measures. (CO2,K2) 4

Answer any one of the following:-

(3.5) Propose a method to improve the accuracy of an existing facial recognition-based security system. (CO3,K3) 4

(3.6) Recommend a biometric authentication model suitable for a mobile banking application and justify your choice. (CO3,K3) 4

Answer any one of the following:-

(3.7) Illustrate the concept of layered security in system architecture and describe its effectiveness in threat mitigation. (CO4,K2) 4

(3.8) Summarize different types of backups and justify their relevance in disaster recovery planning. (CO4,K2) 4

Answer any one of the following:-

(3.9) Explain the contribution of corporate security policies to enforcing governance and accountability. (CO5,K2) 4

(3.10) Propose improvements to WWW policies aimed at reducing risks from unauthorized internet activities. (CO5,K2) 4

SECTION-C 35

4. Answer any one of the following:-

(4.1) Describe cyber security and the role of ethical hackers.(CO1,K2) 7

(4.2) Explain the three main objectives of information security.(CO1, K2) 7

5. Answer any one of the following:-

.

(5.1)	Explain the difference between signature-based and anomaly-based intrusion detection techniques. Discuss their respective advantages and disadvantages. (CO2, K3)	7
(5.2)	Discuss the importance of secure coding practices in application security. Explain key secure coding practices, including input validation, output encoding, and secure error handling.(CO2,K3)	7

6. Answer any one of the following:-

(6.1)	Provide a detailed description of various biometric authentication methods, classifying them as physiological or behavioral. Include a discussion of core biometric traits such as fingerprint, iris, face, signature, and voice. (CO3, K3)	7
(6.2)	Recommend a biometric system for a national identity management project in a developing country. Address design issues, economic considerations, cultural acceptance, and technical feasibility in your proposal. (CO3, K3)	7

7. Answer any one of the following:-

(7.1)	Explain the relationship between information security governance and risk management by discussing their interdependence, functions in corporate policy-making, and their collective role in compliance and accountability. (CO4, K2)	7
(7.2)	Identify and explain all physical security mechanisms applicable to safeguarding IT infrastructure, including their classification and individual contribution to the protection of hardware and data. (CO4, K2)	7

8. Answer any one of the following:-

(8.1)	Develop an implementation plan for publishing and notifying employees about updated security policies in a large organization, incorporating strategies to maximize awareness and compliance.(CO5,K3)	7
(8.2)	Evaluate the effectiveness of current cyber laws in India in addressing modern cybercrimes by analyzing emerging challenges such as ransomware, data theft, and digital impersonation. (CO5,K3)	7