Printed Page:- 03 **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 (2023 - 2024)

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-a. The purpose of an intrusion detection system (IDS) in information security is _____. (CO1) 1

(a) To detect and prevent unauthorized access to information

(b) To encrypt sensitive data

(c) To perform backups of data

(d) To monitor and detect suspicious activity on a network

1-b. _____ is the purpose of input validation in application security. (CO2) 1

(a) Ensuring all user input is stored in a secure database

(b) Enforcing licensing agreements for third-party software

(c) Filtering and sanitizing user input

(d) Encrypting data transmission between the application and the server

1-c. _____ is the most common type of cyber attack. (CO3) 1

(a) Social engineering

(b) Denial-of-service (DoS)

(c) Malware

(d) Phishing

1-d. Which of the following is an example of a physical control in information security?(CO4) 1

(a) Encryption of sensitive data

(b) Implementation of access controls

(c) Use of biometric authentication

(d) Installation of surveillance cameras

1-e. Which section of the Information Technology Act, 2000 deals with the punishment for unauthorized access to a computer system? (CO5) 1

(a) Section 65

(b) Section 42

(c) Section 66

(d) Section 69

2. Attempt all parts:-

2.a.	Write down the three main objectives of information security.(CO1)	2
2.b.	Describe the purpose of input validation in application security.(CO2)	2
2.c.	Explain the risks and benefits of implementing biometric systems in high-security environments such as airports or government facilities. (CO3)	2
2.d.	Explain secure information system. (CO4)	2
2.e.	Explain email spamming/email bombing.(CO5)	2

SECTION-B 20

3. Answer any five of the following:-

3-a.	Describe a secure file transfer protocol (SFTP) and how does it protect data. (CO1)	4
3-b.	Describe the concept of defense in breadth in information security. (CO1)	4
3-c.	Explain backup. Define its type.(CO2)	4
3-d.	Describe backup security measure in detail.(CO2)	4
3.e.	Discuss the advantages and disadvantages of using biometric authentication in terms of user convenience and security.(CO3)	4
3.f.	Define risk management process. (CO4)	4
3.g.	Explain the key components of a security policy.(CO5)	4

SECTION-C 35

4. Answer any one of the following:-

4-a.	Explain encryption with an example and how does it help in information security.(CO1)	7
4-b.	Describe malware in detail and write about are some common types of malware.(CO1)	7

5. Answer any one of the following:-

5-a.	Discuss the concept of secure authentication and authorization in web applications. Explain the potential risks associated with weak authentication mechanisms and inadequate authorization controls.(CO2)	7
5-b.	Explain the role of input validation in application security. Discuss common types of input validation vulnerabilities, such as SQL injection and cross-site scripting (XSS), and explain techniques to mitigate these vulnerabilities. (CO2)	7

6. Answer any one of the following:-

6-a.	Analyze the vulnerabilities and risks of biometric systems to advanced spoofing techniques. (CO3)	7
6-b.	What measures can be implemented to detect and prevent risks of biometric systems to advanced spoofing techniques?(CO3)	7

7. Answer any one of the following:-

7-a.	Explain and differentiate between integrating security at the implementation phase and the developing phase..(CO4)	7
7-b.	Describe the processes of application development security.(CO4)	7

8. Answer any one of the following:-

8-a.	Explain the key steps involved in the policy review process. (CO5)	7

8-b. Explain email security policies in detail. (CO5) 7