R20 Regulation *Subject code:3E7GB*

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

(Autonomous, Accredited by NAAC with 'A+' Grade)

B.Tech VII Semester Regular/Supplementary Examinations, December 2024

INFORMATION SECURITY

(CSE (AI & ML))

Maximum Marks: 70 Date:07.01.2025 Duration: 3 hours

Note: 1.This question paper contains two parts A and B.
2. Part A is compulsory which carries 20 marks. Answer all questions in Part A.
3. Part B consists of 5 Units. Answer any one full question from each unit which carries 10M.
4. Each question carries 10 marks and may have a, b, c, d as sub questions.

Part-A

All the following questions carry equal marks (10X2M=20 Marks)		CO	Bloom Tx
1	Define Information security.	1	I
2	Write about the software attacks?	1	VI
3	Write about the laws and ethics in Information Security?	2	II
4	Identify the different policies in Information Security?	2	III
5	Define the risk control.	3	II
6	Write the risk assessment?	3	II
7	Define public key infrastructure?	4	I
8	Assess the symmetric key cryptography?	4	V
9	What is the purpose of firewall?	5	I
10	Define IDS and IPS.	5	IV

Part-B

Answer All the following questions. (5X10M=50Marks)		CO	Bloom Tx
11	Discuss the various types of threats and attacks on information security, providing examples for each type. [10M]	1	VI
	OR		
12	A. Explain the CNSS security model and its significance in information security. [5M] B. Evaluate the concept of balancing information security and access. Why is it challenging? [5M]	1	II,V
13	A. Explain the components and importance of a Security Education, Training, and Awareness program. [5M] B. Discuss the importance of ethics in information security and explain the codes of ethics of any two professional organizations. [5M]	2	II,VI
	OR		
14	A. Demonstrate the process of creating an information security policy, standards, and practices, and discuss their role in an organization. [5M]	2	II,VI

	B. Elaborate the role of laws and regulations in information security, including relevant U.S. and international laws. [5M]		
15	A. Categorize the risk management process in detail, including risk identification, assessment, and control. [5M] B. Justify the challenges of implementing risk management in information security. [5M]	3	IV,V
	OR		
16	A. Compare and contrast qualitative and quantitative risk management practices. Discuss their advantages and disadvantages. [5M] B. Explain the different risk control practices and provide examples of each. [5M]	3	II,II
17	Recommend the evolution of encryption, highlighting the differences between early codes and modern cryptographic techniques. [10M]	4	IV
	OR		
18	A. Demonstrate the structure and function of Public Key Infrastructure (PKI) and its role in secure communication. [5M] B. Discuss symmetric-key cryptography and public-key cryptography, comparing their strengths and limitations. [5M]	4	II,VI
19	A. Explain the challenges and strategies involved in maintaining security within an organization's information systems. [5M] B. Examine digital forensics, its process, and its significance in information security. [5M]	5	II,IV
	OR		
20	Classify the different types of security technology tools, including access controls, firewalls, VPNs, and intrusion detection and prevention systems. [10M]	5	IV