2/101 **2411N829** Candidate's Seat No :_____

IMSc (CSF) (NEP) Sem.-5 Examination

DSC-C-ICSF-353T

AI in Cyber Security

Time : 2-00 Hours] **November-2025** **[Max. Marks : 50**

Question 1: Answer the following questions:

i. Differentiate between Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL). 5 Marks

ii. Explain the Machine Learning lifecycle step by step. 5Marks

OR

i. Write a short note on AI Ethics with examples of bias or privacy. 5Marks

ii. Describe the history of AI with key milestones from 1950 to present. 5Marks

Question 2: Answer the following questions:

i. Differentiate between Classification and Regression. 5Marks

ii. Explain the difference between TP, FP, TN, FN with real-world examples 5Marks

OR

i. What is K-Nearest Neighbors (KNN)? Explain it with an example. 5Marks

ii. Explain Linear Regression with a suitable example. 5Marks

Question 3: Answer the following questions:

i. Explain the architecture and working of a Convolutional Neural Network. 5Marks

ii. Describe the training process in neural networks including forward propagation, backpropagation, and optimization. 5Marks

OR

i. Explain the architecture and working of a Recurrent Neural Network (RNN). 5Marks

ii. Discuss applications of Deep Learning in cybersecurity with specific examples. 5Marks

Question 4: Answer the following questions:

i. Explain how AI detects polymorphic malware, deepfakes, or phishing attacks 5Marks

ii. Discuss the increasing sophistication of cyber attacks with examples of Advanced Persistent Threats (APTs) and AI-driven attacks. 5Marks

OR

P.T.O

N829-2

i. Discuss various types of cyber attacks including APTs, AI-driven attacks, deepfakes, supply chain attacks, and polymorphic malware. 5Marks

ii. Discuss the need for more skilled cybersecurity professionals and how AI and ML will help combat cyber threats in the future. 5Marks

Question 5: Attempt any ten out of twelve. 10 Marks

1. Which year did the term "Artificial Intelligence" get coined at the Dartmouth Conference?
2. Which AI application helps in understanding and generating human language?
3. Which milestone showcased strategic AI by defeating a Go champion?
4. Which approach follows IF–THEN rules?
5. The goal of AI ethics includes: _____.
6. In AI/ML for cybersecurity, phishing detection uses: _____.
7. The Sigmoid activation function outputs values in the range: _____.
8. In CNNs, pooling layers are used for: _____.
9. GANs (Generative Adversarial Networks) consist of: _____.
10 High cost of cybersecurity breaches includes: _____.
11 Behavioural biometrics in access control can detect: _____.
12 AI ethics and regulation in cybersecurity focuses on: _____.

.....X.....X.....