CURRICULUM FRAMEWORK FOR THREE YEAR UG DEGREE / FOUR YEAR UG DEGREE (HONOURS) / FOUR YEAR UG DEGREE (HONOURS WITH RESEARCH)

Value Added Course (VAC) for UG Programme

Department of Computer Science

North Lakhimpur University

(As approved by Board of Studies in Computer Science held on 18th June 2026 and passed by Academic Council held on .....)

Course Code	**:**	**VAC1**
Course Title	**:**	**INTRODUCTION TO ARTIFICIAL INTELLIGENCE**
Nature of the Course	**:**	**VAC**
Total Credit assigned	**:**	**2**
Component of the Course	**:**	**Lecture: 2 Practical: 0 Tutorial: 0**
Distribution of Marks	**:**	**End Semester: 28 In Semester: 12**

Course Objectives:

The main objectives of this course are:

Objective-1. Explain the fundamental concepts, evolution, types and applications of Artificial Intelligence.

Objective -2. Describe intelligent agents, AI environments, problem characteristics and basic search techniques.

Objective -3. Identify suitable AI/ML domains and techniques for solving problems in different contexts.

Objective -4. Analyze AI case studies and evaluate the suitability of AI-based solutions across application domains.

Course Content

Unit	Content	Marks	L	P	T
I	Introduction to AI • Concept of Artificial Intelligence • Evolution and types of AI • Introduction to intelligent agents and types of AI agents • Rationality of agents; AI environment and its types • Problem characteristics in AI • Introduction to search techniques • Uninformed and informed search	11	12	0	0
II	Introduction to Major Domains of AI • Concept of Machine Learning • Natural Language Processing • Computer Vision • Robotics • Expert Systems • Generative AI • Applications of AI across various domains	11	10	0	0
III	Case Studies • Applications of AI in healthcare • Applications of AI in entertainment • Applications of AI in education • Applications of AI in agriculture • Applications of AI in gaming and other domains	6	8	0	0
Total		**28**	**30**	**0**	**0**

Mode of In-Semester assessment (12 Marks):

A. Sessional Activity

B. Sessional Tests: (two Sessional Tests)

Sessional activity:

1. AI Concept Review Task

• Prepare a short note or quiz response on AI concepts, types, intelligent agents, and AI environments.

2. AI Domain Identification Task
• Identify suitable AI/ML domains such as ML, NLP, computer vision, robotics, expert systems, or generative AI for given real-life problems.

3. Case Study Analysis Task
• Analyse an AI case study from healthcare, education, agriculture, entertainment, or gaming and justify the AI technique used.

Evaluation Criteria:
• Correct understanding of AI concepts and terminology.
• Ability to match AI/ML techniques with suitable problem contexts.
• Clarity of case-study analysis and justification.
• Quality of explanation, presentation, and conclusion.

Expected Course Learning Outcomes:

By the end of the course, students will be able to:

CLO-1. Explain the concept, evolution, types, agents, environments and problem characteristics of Artificial Intelligence.

CLO-2. Apply basic AI problem-solving and search concepts to identify suitable AI techniques for given problems.

CLO-3. Compare major AI domains such as Machine Learning, NLP, Computer Vision, Robotics, Expert Systems and Generative AI.

CLO-4. Relate AI case studies and categorize the suitability of AI-based solutions in different application domains.

Cognitive Map of Course Learning Outcomes based on Revised Bloom's Taxonomy

Knowledge Dimension	Remember	Understand	Apply	Analyse	Evaluate	Create
Factual Knowledge	CLO1	CLO1				
Conceptual Knowledge		CLO1, CLO2	CLO2	CLO3		
Procedural Knowledge			CLO2, CLO3	CLO3, CLO4		
Metacognitive Knowledge						

Mapping of CLO with Programme Specific Outcomes (PSOs)

CLO / PSO	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CLO1	2								1	
CLO2		2		1						
CLO3	1	1							1	
C;O4		2			1					1
Average Contribution	**0.75**	**1.25**		**0.25**	**0.25**				**0.5**	**0.25**

Scale: 3 = High contribution, 2 = Moderate contribution, 1 = Low contribution; blank = No direct mapping.

Suggested readings:

1. Rich, E., & Knight, K. (1991). Artificial intelligence (2nd ed.). Tata McGraw-Hill.
2. Patterson, D. W. (2007). Introduction to AI and expert systems. PHI Learning.
3. Mitchell, T. M. (2013). Machine learning. Tata McGraw-Hill Education.
4. Bishop, C. M. (2007). Pattern recognition and machine learning. Springer.

Course Code	**:**	**VAC2**
Course Title	**:**	**INTRODUCTION TO CYBER SECURITY**
Nature of the Course	**:**	**VAC**
Total Credit assigned	**:**	**2**
Component of the Course	**:**	**Lecture: 2 Practical: 0 Tutorial: 0**
Distribution of Marks	**:**	**End Semester: 28 In Semester: 12**

Course Objectives:

The main objectives of this course are:

Objective -1. Explain the basic concepts of cyber security, cyberspace and the digital ecosystem.

Objective -2. Identify common cyber threats, vulnerabilities, attacks and online risks.

Objective -3. Apply safe and responsible practices while using digital platforms, social media, e-mail, mobile apps and online services.

Objective -4. Analyze cyber ethics, privacy, data protection, cyber laws and cyber-crime reporting mechanisms in responsible digital contexts.

Course Content

Unit	Content	Marks	L	P	T
I	Introduction to Cyber Security • Overview of computer and web technology • Origin of the Internet, World Wide Web, and web browsers • Meaning of cyberspace and digital ecosystem • Importance of cyber security in daily life • Types of cyber threats • Basic concepts: vulnerability, threat, attack, and risk • Overview of cyber security domains	8	8	0	0
II	Cyber Threats and Protection Mechanisms • Common cyber threats: malware, virus, worm, trojan, ransomware • Phishing, social engineering, identity theft, and online fraud • Password security and authentication methods • Safe browsing practices • Secure use of social media and email • Basic security tools: antivirus software, firewalls, and two-factor authentication	10	11	0	0
III	Cyber Ethics, Laws and Safe Digital Practices • Cyber ethics and responsible digital behaviour • Privacy and data protection • Digital footprints and online reputation • Introduction to cyber laws in India: Information Technology Act, 2000 • Reporting cyber crimes through national portals such as cybercrime.gov.in • Safe use of mobile apps and online transactions • Role of individuals in cyber safety	10	11	0	0
Total		**28**	**30**	**0**	**0**

Mode of In-Semester assessment (12 Marks):

A. Sessional Activity

B. Sessional Tests: (two Sessional Tests)

Sessional activity:

1. Cyber Security Concept Task

• Prepare a short note or quiz response on cyberspace, digital ecosystem, threats, vulnerabilities, attacks, and risks.

2. Threat Identification Task

• Identify phishing, malware, identity theft, and social engineering cases from sample scenarios.

3. Safe Digital Practice Task

• Prepare a checklist for password safety, two-factor authentication, safe browsing, secure email/social media use, and mobile app safety.

4. Cyber Ethics and Law Awareness Task

• Explain privacy, digital footprints, ethical use, cyber laws, and the process of reporting cyber crimes.

Evaluation Criteria:

• Correct understanding of cyber security concepts and terminology.
• Ability to identify online risks and cyber threats from examples.
• Application of safe digital practices and basic protection mechanisms.
• Awareness of ethical, legal, and reporting responsibilities.

Expected Course Learning Outcomes:

By the end of the course, students will be able to:

CLO-1. Explain fundamental concepts of cyber security, cyberspace, digital ecosystem, threats, vulnerabilities, attacks and risks.

CLO-2. Identify common cyber threats including malware, phishing, social engineering, identity theft and online fraud.

CLO-3. Apply safe digital practices related to passwords, authentication, browsing, e-mail, social media, mobile apps, online transactions and security tools.

CLO-4. Analyze privacy, data protection, digital footprints, cyber ethics, cyber laws and cyber-crime reporting responsibilities.

Cognitive Map of Course Learning Outcomes based on Revised Bloom's Taxonomy

Knowledge Dimension	Remember	Understand	Apply	Analyse	Evaluate	Create
Factual Knowledge	CLO1	CLO1				
Conceptual Knowledge		CLO1, CLO2	CLO2	CLO3		
Procedural Knowledge			CLO2, CLO3	CLO3, CLO4		
Metacognitive Knowledge						

Mapping of CLO with Programme Specific Outcomes (PSOs)

CLO / PSO	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CLO1	1				2				1	
CLO2		2			2					
CLO3				2	2					
CLO4		2			3					1
Average Contribution	**0.25**	**1**		**0.5**	**2.25**				**0.25**	**0.25**

Scale: 3 = High contribution, 2 = Moderate contribution, 1 = Low contribution; blank = No direct mapping.

Suggested readings:

1. Pandey, J. (n.d.). Introduction to cyber security. Sage Publications.
2. Dhar, P. (n.d.). Fundamentals of information technology in business. Abhijay Publication.
3. Sinha, P. K. (n.d.). Fundamentals of computer and IT.
4. Sarkar, A., Santra, S., & Jana, S. (n.d.). Basics of cyber security. U. N. Dhur & Sons (P) Ltd.