KLS Vishwanathrao Deshpande Institute of Technology,Haliyal

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING(AI&ML)

Semester:IV **Year:2025-2026**

CourseTitle	Foundation of Cyber Security in AI.	**Course Code**	ADDON
Total Teaching Hours	30	Teaching + Tutorial Hours/Week	3
Internal Assessment Marks	05		
Course Plan Prepared by	Prof.Bheerappa	Date	02-02-2026

Course Content(Syllabus)

MODULE-1 **Introduction to AI & Security Fundamentals** Defining AI Security (protecting AI) vs. AI for Security (using AI to protect). • Key Concepts: CIA Triad (Confidentiality, Integrity, Availability) in AI. • AI Overview: Machine Learningvs.Deep Learning,Supervised vs.Unsupervised Learning.•Threat Landscape:Traditional threatsvs.AI-powered threats.	10 Hrs
MODULE-2 **AI for Security - Threat Detection.Anomaly Detection and Behavioral Analysis:** Applications: Using AI for network intrusion detection (IDS/IPS), malware classification, and user behavior analytics (UEBA).	10 Hrs
MODULE-3 **Adversarial Machine Learning– Attacks:** Vulnerabilities in ML pipelines. • Attack Types: Evasion attacks (input manipulation), Poisoning attacks (data tampering), Model Extraction/Inversion attacks. • Techniques: Gradient-based attacks (FGSM, PGD), White-box vs. Black-box threats	10 Hrs

Staff Handling:Prof.Bheerappa Sasanoor

Course out comes:

CO1:Understand AI fundamentals and security principles including CIA triad.

CO2:Apply ML/DL techniques for threat detection and behavioral analysis.

CO3:Analyze traditional and AI-powered threats in cyber security.

CO4:Design and implement AI-based security applications using modern tools