NIRMA UNIVERSITY

Institute:	Institute of Technology, School of Technology
Name of Programme:	MTech CSE (Cyber Security), MTech CSE (Data Science)
Course Code:	6CS263ME25
Course Title:	Data Privacy
Course Type:	Department Elective-III
Year of Introduction:	2025-26

L	T	Practical Component				C
		LPW	PW	W	S	
3	0	2	-	-	-	4

Course Learning Outcomes (CLO):

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

1. explain the concepts of web security and privacy, hardware and software vulnerabilities (BL2)
2. apply privacy-preserving models and techniques (BL3)
3. assess the emerging technologies for data privacy and protection. (BL5)
4. evaluate the case studies of data privacy breaches. (BL5)

Unit	Contents	Teaching Hours (Total 45)
Unit-I	**Introduction to Security and Privacy:** Cryptographic Primitives, Web security, Hardware and software vulnerabilities, Social and legal Aspect of privacy and privacy regulations	10
Unit-II	**Privacy Concepts and Models:** Data localization issues, Managing personally identifiable or sensitive information, Data Consent, Anonymization models: K-anonymity, l-diversity, t-closeness, differential privacy, Privacy-preserving techniques	12
Unit-III	**Protection Models:** Basic concepts and definitions, objectives, disclosure control and inference of entities, models of protection like null map, k-map, wrong-map	08
Unit-IV	**Demographics and Uniqueness**: Data linking, data profiling, data privacy attacks	06
Unit-V	**Emerging Applications** and **Case Studies:** AI for Privacy, the role of federated learning and blockchain in data privacy.	09

Self-Study:

The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study content.

Suggested Readings/ References:

1. Vicenc Torra, Guide to Data Privacy: Models, Technologies and Solutions, Springer
2. Stallings, W. Cryptography and Network Security, Pearson
3. Giannotti, F., & Pedreschi, D., Mobility, data mining and privacy: Geographic knowledge discovery, Springer Science & Business Media
4. Bygrave, L. A. Data privacy law: an international perspective, Oxford: Oxford University Press
5. Scoble, R., Israel, S., & Benioff, M. R. Age of context: Mobile, sensors, data and the future of privacy. USA: Patrick Brewster Press
6. Bendat, J. S., & Piersol, A. G. Random data analysis and measurement procedures, Wiley.

Suggested List of Experiments:

Sr. No.	Name of Experiments/Exercises	Hours
1	a. Exposure to network and security-related Linux commands in Kali Linux OS.	04
	b. Study of Stack and Buffer Overflow attack	
2	a. Installation and exploring Openssl- Encryption/Decryption algorithms	04
	b. Hashing and Digital Signature generation in Openssl	
3	Certificate authority creation and installation using OpenSSL.	02
4	a. Network Mapper (NMAP) tool for port vulnerability assessment.	04
	b. Installation of Kali Linux using VMware and installing of toolkits for phishing and DoS attacks	
5	MetaExploit and Burp Suite tool for various vulnerability assessments.	06
6	Implement SQL injection attack on a target system	04
7	Implement machine learning algorithms with built-in privacy-preserving techniques like Differential Privacy (DP) or Federated Learning (FL).	06