NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	MTech CSE (Cyber Security)
Course Code:	6CS404
Course Title:	Data Privacy
Course Type:	(√ **Core**/ □ Value Added Course / □ Department Elective / □ Institute Elective/ □ University Elective/ □ Open Elective / □ Any other)
Year of Introduction:	2022-23

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

Course Learning Outcomes (CLOs):

At the end of the course, the student will be able to –

1. explain the concepts of web security and privacy, hardware and software vulnerabilities and protection mechanisms (BL2)
2. make use of the protection mechanisms against several data-related attacks (BL3)
3. infer the need for data privacy and the related technologies (BL4)
4. determine the requirements of attacks and secure data sharing practices with privacy preservation policies (BL5)

Syllabus: **Total Teaching hours: 45**

Unit	**Syllabus**	**Teaching hours**
Unit-I	**Introduction to Security:** Cryptography Basics, Web security considerations, Protocols- SSL/TLS, SET, Secure Shell, Hardware vulnerabilities- Backdoor, Hardware Trojans, Software vulnerabilities: Buffer Overflow, XSS, SQL injection, Prevention and Counter Measures	07
Unit-II	**Privacy Preservation Schemes:** Data localization issues, Managing personally identifiable or sensitive information, Hippocratic databases, Homomorphic Encryption, Identity-Based Encryption, Differential privacy, Privacy-preserving data analysis	12
Unit-III	**Disclosure Control:** Introduction, Data Quality vs. Anonymity, Data linkage, Disclosure Control Techniques, Data Anonymization-Formal Analysis, Models of Protection- null map, k-map, wrong-map	10
Unit-IV	**Data Explosion**: Availability vs. Storage vs. Collection Trade-off, Barriers to distribution, Mathematical models for sharing practices and policies for computing privacy and risk measurements	08
Unit-V	**Mechanisms of Backup and Disaster Recovery Tools:** Backup Mechanisms- Restor points, Failover, Failback, Data Replication, Disaster recovery tools: Carbonite, Arcserve, Veritas, Recent Data Privacy Use Cases: Healthcare, Internet of Vehicles	08

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

Suggested Readings/ References:

1. Stallings, W. Cryptography and Network Security, Pearson Education India.
2. Giannotti, F., & Pedreschi, D. (Eds.). Mobility, data mining and privacy: Geographic knowledge discovery, Springer Science & Business Media.
3. Bygrave, L. A. Data privacy law: an international perspective (Vol. 63), Oxford: Oxford University Press.
4. Scoble, R., Israel, S., & Benioff, M. R. Age of context: Mobile, sensors, data and the future of privacy. USA: Patrick Brewster Press. Bendat, J. S., & Piersol, A. G. Random data analysis and measurement procedures, Wiley

Suggested List of Experiments:

Sr. No.	Title	Hours
1	Installation and Study of Openssl-Encryption/Decryption algorithms	02
2	Hashing and Digital Signature generation in Openssl	02
3	Certificate authority creation and installation using Openssl.	04
4	Installation of Kali Linux using VMware and installing of toolkits for phishing and DoS attacks,	02
5	Demonstrate the working of various disaster recovery tools	04
6	Study and perform stack and buffer overflow attacks.	04
7	Installation of backdoor through the Metasploitable 2 console on a target system	04
8	Analyze SYN flooding attacks through Low orbit ION Cannon tool	04
9	Implement SQL Injection attack on a target system, and possible secure practices to prevent SQL injection	02
10	Develop secure coding practices to handle Code Injection Vulnerabilities such as SQL Injection, PHP Injection and Command Injection	02