COURSE CONTENT

CYBER SECURITY								
II Semester: CSE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
2525813	**Foundation**	3	0	0	3	40	60	100
Contact Classes: 45	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 45**		
Prerequisites: Understanding of operating system concepts**.**								

Course Overview:

This course focused on protecting computer systems, networks, applications, and data from unauthorized access, attacks, and damage. As digital infrastructure grows, cyber threats become more sophisticated, making security knowledge essential for designing resilient systems.

Course Objectives:

1. To understand the fundamentals of cyber security, cyber threats, and attack mechanisms.
2. To study cyber laws, cyber ethics, and digital forensic investigation techniques.
3. To analyze security challenges in mobile, wireless, and networked computing environments.
4. To evaluate organizational security risks, privacy issues, and cybercrime impacts on digital systems.
5. To develop defensive strategies and security policies for protecting information systems and sensitive data.

Course Outcomes: After Completion of the Course, Students should be able to

1. Design cyber security concepts and threat models for secure communication systems in protecting organizational assets.
2. Analyze cyber laws, policies, and digital forensic techniques to investigate cybercrimes in preserving admissible digital evidence.
3. Evaluate mobile and wireless device vulnerabilities to recommend effective authentication and security policies in enterprise environments.
4. Examine organizational implications of cyber threats to formulate strategies mitigating risks in web services, social media, and intellectual property.
5. Develop privacy-preserving solutions and policies for sensitive domains such as healthcare and financial systems through real-world case analysis.

UNIT - I: Introduction to Cyber Security: Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy.

UNIT - II: Cyberspace and the Law & Cyber Forensics: Introduction, Cyber Security Regulations, Roles of International Law. The INDIAN Cyberspace, National Cyber Security Policy. Introduction, Historical background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber Forensics and Digital evidence, Forensics Analysis of Email, Digital Forensics Lifecycle, Forensics Investigation, Challenges in Computer Forensics

UNIT - III: Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication service Security, Attacks on Mobile/Cell Phones, Organizational security Policies and Measures in Mobile Computing Era, Laptops.

UNIT - IV: **Cyber Security: Organizational Implications:** Introduction, cost of cybercrimes and IPR issues, web threats for organizations, security and privacy implications, social media marketing: security risks and perils for organizations, social computing and the associated challenges for organizations

UNIT - V: Privacy Issues: Basic Data Privacy Concepts: Fundamental Concepts, Data Privacy Attacks, Data linking and profiling, privacy policies and their specifications, privacy policy languages, privacy in different domains- medical, financial, etc. Cybercrime: Examples and Mini-Cases

Examples: Official Website of Maharashtra Government Hacked, Indian Banks Lose Millions of Rupees, Parliament Attack, Pune City Police Bust Nigerian Racket, e-mail spoofing instances.

Mini-Cases: The Indian Case of online Gambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.

TEXT BOOKS:

1. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley.
2. B.B. Gupta, D.P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335,2018.

REFERENCE BOOKS:

1. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
2. Introduction to Cyber Security, Chwan-Hwa(john) Wu,J. David Irwin, CRC Press T&FGroup.

ELECTRONIC RESOURCES:

1. https://www.coursera.org/specializations/cyber-security
2. https://www.sanfoundry.com/certification/cyber-security-certification/
3. https://www.udemy.com/topic/cyber-security/
4. https://www.edx.org/learn/cybersecurity/

MATERIALS ONLINE:

1. Course template
2. Tutorial question bank
3. Tech talk and Concept Video topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. E-Learning Readiness Videos (ELRV)