		L	T	P	C
		3	0	0	3

CYBER SECURITY
(Open Elective-III)

Course Objectives:

The Cyber security Course will provide the students with foundational Cyber Security principles, Security architecture, risk management, attacks, incidents, and emerging IT and IS technologies. Students will gain insight into the importance of Cyber Security and the integral role of Cyber Security professionals.

Course Outcomes:

By the end of the course, student will be able to

- Understand Cyber Security architecture principles
- Identifying System and application security threats and vulnerabilities
- Identifying different classes of attacks
- Cyber Security incidents to apply appropriate response
- Describing risk management processes and practices
- Evaluation of decision making outcomes of Cyber Security scenarios

UNIT-I: Introduction to Cybercrime: Introduction, Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Cybercriminals, Classifications of Cybercrimes, Cybercrime: The Legal Perspectives, Cybercrimes: An Indian Perspective, Cybercrime and the Indian ITA 2000, A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens

Cyber Offenses: Planning of Offenses by Cyber Criminals–Introduction, Planning attacks by criminals, Social Engineering, Cyber stalking, Cyber cafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector Cloud Computing.

UNIT-II: 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, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops.

UNIT-III: Tools and Methods used in Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks, Phishing and Identity Theft: Introduction, Phishing, Identity Theft (ID Theft)

UNIT-IV: Cybercrimes and Cyber Security: Need for Cyber laws: The Indian Context, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Consequences of Not Addressing the Weakness in Information Technology Act, Digital Signatures and the Indian IT Act, Information Security Planning and Governance, Information Security Policy Standards, Practices, The information Security Blueprint, Security education, Training and awareness program, Continuing Strategies.

UNIT-V: Understanding Computer Forensics: Introduction, Historical Background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber forensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation, Computer Forensics and Steganography, Relevance of the OSI 7 Layer Model to Computer Forensics, Forensics and Social Networking Sites: The Security/Privacy Threats, Computer Forensics from Compliance Perspective, Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing, Antiforensics

Text Books:

1. Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Nina Godbole, Sunit Belapure, Wiley.

Reference Books:

1. Principles of Information Security, Micheal E.Whitman and Herbert J.Mattord, Cengage Learning.
2. Information Security, Mark Rhodes, Ousley, MGH.