GUJARAT TECHNOLOGICAL UNIVERSITY

B.Pharm

SEMESTER: VII

Subject Name: Cyber Security
Subject Code: 2270006

Teaching Scheme				Evaluation Scheme			
Theory	Tutorial	Practical	Total	Theory		Practical	
				External	Internal	External	Internal
3	0	0	3	80	20	0	0

No	Course Content	Hrs
1	**Introduction to Cybercrime** Definition and Origins of the Word, Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes: E-Mail Spoofing, Spamming, Cyber defamation, Internet Time Theft, Salami Attack/Salami Technique, Data Diddling, Forgery, Web Jacking, Newsgroup Spam/Crimes Emanating from Usenet Newsgroup, Industrial Spying/Industrial Espionage, Hacking, Online Frauds, Pornographic Offenses , Software Piracy, Computer Sabotage, E-Mail Bombing/Mail Bombs, Usenet Newsgroup as the Source of Cybercrimes , Computer Network Intrusions, Password Sniffing, Credit Card Frauds, Identity Theft	7
2	**Cyberoffenses and Law** Introduction, Categories of Cybercrime, How Criminals Plan the Attacks: Reconnaissance, Passive Attack, Active Attacks, Scanning/Scrutinizing gathered Information, Attack (Gaining and Maintaining the System Access), Social Engineering-Classification of Social Engineering, Cyber stalking: Types of Stalkers, Cases Reported on Cyber stalking, How Stalking Works? Cyber cafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing: Why Cloud Computing? Types of Services, Cybercrime and Cloud Computing. Attacks on mobile devices. Recognizing and Defining Computer Crime, Contemporary Crimes, Computers as Targets, Contaminants and Destruction of Data, Security Policies, WWW policies, Email Security policies, Information Security Standards-ISO, Copyright Act, Patent Law, IPR. Cyber Laws in India; IT Act 2000 Provisions, Intellectual Property Law: Copy Right Law, Software License, Semiconductor Law and Patent Law	11
3	**Network Defense tools** Firewalls and Packet Filters: Firewall Basics, How a Firewall Protects a Network, basic of Virtual Private Networks, Linux Firewall, Windows Firewall, Snort: intrusion detection system	5
4	**Cybercrime: Mobile and Wireless Devices** Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era: Types and Techniques of Credit Card Frauds, Security Challenges Posed by Mobile Devices Attacks on Mobile/Cell Phones: Mobile Phone Theft, Mobile Viruses, Mishing, Vishing, Smishing, Hacking Bluetooth, Mobile Devices: Security Implications for	10

	Organizations: Managing Diversity and Proliferation of Hand-Held Devices, Unconventional/Stealth Storage Devices Threats through Lost and Stolen Devices, Protecting Data on Lost Devices, Educating the Laptop Users Organizational Measures for Handling Mobile Devices-Related Security Issues: Encrypting Organizational Databases, Including Mobile Devices in Security Strategy, Organizational Security Policies and Measures in Mobile Computing Era: Importance of Security Policies relating to Mobile Computing Devices, Operating Guidelines for Implementing Mobile Device Security Policies, Organizational Policies for the Use of Mobile Hand-Held Devices, Laptops: Physical Security Countermeasures	
5	**Introduction to Cyber Crime Investigation** assword Cracking, Keyloggers and Spyware, Virus and Warms, Trojan and backdoors, Steganography, DoS and DDoS attack, SQL injection, Buffer Overflow, Attack on wireless Networks.	5
6	**Organizational and Cybersecurity**: Introduction to implications of insider, outsider attacks, Cost of cybercrimes and IPR issues, overview of webthreats to organizations, security and privacy implications from Cloud Computing, Over view of Social media : use, security risks and peril for organization	7

References Books:

1. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole and Sunit Belpure, Publication Wiley.
2. Anti-Hacker Tool Kit (Indian Edition) by Mike Shema, Publication Mc Graw Hill.