SARDAR PATEL UNIVERSITY
Programme & Subject: M.Sc – Information Technology (Integrated)
Semester: IV
Syllabus with Effect from: June-2013

Paper Code: PS04EIIT01	**Total Credit: 2**
Title Of Paper: Cyber Security	

Unit	Description in detail	Weightage (%)
I	**Introduction to Cybercrime** Introduction, 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, Data Diddling, Forgery, Web Jacking, Hacking, Online Frauds, Software Piracy, Computer Sabotage, E-Mail Bombing/Mail Bombs, and Computer. Network Intrusions, Password Shiffing, Credit Card Frouds, Identify Theft.	25%
II	**Cyber offenses** Introduction, Categories of Cybercrime How Criminals Plan the Attacks: Reconnaissance, Passive Attack, Active Attacks, Attack (Gaining and Maintaining the System Access) Cyberstalking: Types of Stalkers, Cases Reported on Cyberstalking, How Stalking Works? Real-Life Incident of Cyberstalking. Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Botnet Attack Vector Cloud Computing: Why Cloud Computing? , Types of Services, Cybercrime and Cloud Computing	25%
III	**Cybercrime: Mobile and Wireless Devices** Proliferation ofMobile and Wireless Devices. Trends in Mobility. Security Challenges Posed byMobile Devices. Registry Settings forMobile Devices Attacks on Mobile/Cell Phones: Mobile Phone Theft, Mobile Viruses, Mishing, Vishing, Smishing, Hacking Bluetooth. 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.	25%
IV	**Cybercrime: Tools and Methods** Proxy Servers and Anonymizers, Phishing: How Phishing Works? Password Cracking: Online Attacks, Offline Attacks, Strong, Weak and Random	25%

	Passwords, Random Passwords. Key loggers and Spy wares: Software Keyloggers, Hardware Keyloggers, Antikeylogger, Spywares. Virus and Worms: Types of Viruses. Trojan Horses and Backdoors: Backdoor, How to Protect from Trojan Horses and Backdoors. DoS and DDoS Attacks: DoS Attacks, Classification of DoS Attacks, Types or Levels of DoS Attacks, Tools Used to Launch DoS Attack, DDoS Attacks, How to Protect from DoS/DDoS Attacks. SQL Injection: Steps for SQL Injection Attack, How to Avoid SQL Injection Attacks. Buffer Overflow: Types of Buffer Overflow, How to Minimize Buffer Overflow.	

Basic Text & Reference Books:-

- Nina Godbole, Sunit Belapur, "Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley India Publications, April, 2011