BCA308 Cyber Ethics	
Teaching Scheme Lectures: 3 hrs/Week Tutorials: 1 hr/Week Credits: 4	**Examination Scheme** Class Test – 12 Marks Teachers Assessment – 6 Marks Attendance – 12 Marks End Semester Exam – 70 Marks

Prerequisite: Data & Network Security

Course Objectives:

1. The students will understand the importance of professional practice, Law and Ethics in their personal lives and professional careers.
2. The students will learn the rights and responsibilities as an employee, team member and a global citizen

Detailed Syllabus:

Unit-1 **Cyber Crime:** Definition and Origin of the Word, Cyber Crime and Information Security, Who are Cyber Criminals, Classification of Cybercrimes, E-mail Spoofing, Cyber Defamation, Internet Time Theft, Salami Attack, Salami technique Data Diddling, Forgery, Web Jacking, Newsgroup Spam, Industrial Spying, Hacking, Online Frauds, Pornographic Offenders, Software Piracy, Computer Sabotage Email Bombing, Computer Network Intrusion, Password Sniffing, Credit Card Frauds, Identity Theft.
Unit-2 **Cyber Offenses:** How Criminals plan them, Categories of Cyber Crimes, How Criminal Plans the Attack: Active Attacks, Passive Attacks, , Social Engineering, Classification of Social Engineering, Cyber Stalking : types of Stalkers, Cyber Cafe and Cyber Crimes, Botnets , Attack Vectors, Cyber Crime and Cloud Computing.
Unit-3 **Cyber Crime:** The Legal Perspectives, The Cyber Crime Indian Perspectives, The Cyber Crime And Indian ITA 2000/2001, Hacking and Indian Laws, Global Perspective on Cyber Crime , Cyber Crime and extended Enterprise.
Unit-4 **Tools and Methods used in Cybercrime:** Proxy server and Anonymizers, phishing: How Phishing works? How password cracking works? Keylogers and Spywares, Virus and Worms, Trozan Horses and Backoors, Dos and Ddos Attacks, SQL Injection, Buffer Overflow, An Attacks on Wireless Networks
Unit-5 **Phishing and Identity Theft: Phishing:** Methods of Phishing, Phishing Techniques, Types of Phishing Scams, Phishing countermeasures, Identity theft, Types and Techniques of identity thefts and its counter measures.
Unit-6 **Understanding Computer Forensics:** Digital forensic Science, Need for Computer Foransic, Cyber Forensic and digital Evidence and rules of Evidence, Forensics Analysis of E-Mail, Digital Forensic Life Cycle.

References:

1. Cyber Security: Understanding Cyber Crimes , Computer Forensics and Legal Perspectives By Nina Godbole, SunitBelapur , Wiley.
2. Debby Russell and Sr. G. T Gangemi, "Computer Security Basics (Paperback), 2nd Edition, O Reilly Media.
3. Thomas R. Peltier, Information Security policies and procedures: A Practitioners Reference, 2nd Edition Prentice Hall

Course Outcomes:

After completing the course, students will be able to:

1. To identify and describe the major types of cybercrime.
2. To identify cybercrime vulnerabilities and exploitations of the Internet.
3. Identify various classifications of cybercrimes and cyber-criminals.
4. To identify appropriate responses to cyber-criminal activity.
5. To understand the law with regards to the investigation and prosecution of cyber criminals.
6. To identify appropriate law enforcement strategies to both prevent and control cybercrime.
7. Explain jurisdictional challenges that nations face when responding to cybercrime