

Branch Name:	Other than Computer Engineering / Information Technology
Semester/Year:	Semester V / Third Year
Subject Title:	Cyber Law and Ethics (Open Elective)
Subject Code:	1ET1030506
Pre-requisite:	Basics of knowledge of computer and Information technology.

Course Objective:

- The main objective of this course is to make the students aware regarding problem formulation and transforming human readable steps into suitable in cyber world.
- The course also intends to prepare the students aware about the uses of internet as well as activity going in the daily crime in internet
- Other track of the course focuses on the challenges to Indian laws and cybercrime scenario in India and punishment toward the referred crimes.

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture (L)	Tutorial (T)	Practical (P)	Credit	Theory (Marks)		Practical (Marks)		Total (Marks)
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
01	-	02	02	35	15	30	20	100

Subject Contents			
Sr. No	Topic	Total Hours	Weightage (%)
01	Evolution and growth of ICT: Introduction, information, communication, fundamental of software and hardware network, types of network, topology, Internet and e-commerce.	2	15
02	Fundamental of Cyber Crime: Introduction to Cyber laws in India, computer crime, cybercrime, classification of cybercrimes, cyber-criminal, A Case Study: current trends in cyber-attacks, fundamental of Data exclusivity laws.	2	15
03	Mobile and Wireless Devices in Cyber Crime: Introduction, proliferation of mobile and Wireless device, trends immobility, Attacks on wireless networks, Attack on mobile/cell phone, mobile device: security implication for organization.	3	20
04	Cyber Crime Tools and Techniques: introduction, proxy server and anonymizers, phishing, password cracking, keylogger and spywares, virus and worms, Trojan horses and backdoor, steganography, DoS and DDoS Attacks, SQL injection, Buffer overflow.	4	30
05	Legal Perspective of Cyber Security: Introduction, cyber crime and the legal landscape around the world, the Indian IT act, challenges to Indian laws and cyber crime scenario in India, digital signature and the Indian IT act, amendments to Indian IT Act., cyber crime and punishment.	3	20

Course Outcome:

Upon completion of this course, students will be able to:

- Understand the meaning and different forms of ICT
- Realize the activities carried using forensic technologies in detection of cyber crime
- Understand the core concepts of defensive and offensive security.
- Cyber Crime Cases and IT act of India and amendments.
- Relate the laws enforced by the judiciary to handle cybercrimes and cyber frauds

List of Text Books:

1. Cyber security: Understanding Cyber crime Computer Forensics and Legal Perspectives By Nina Godbole & Sunit Belapure, WILEY
2. Cyber laws by C.K.Punia
3. Data and computer communication, William Stallings, Pearson

List of Reference Books:

1. Cyber laws and IT protection by Harish Chander.
2. Cyber Forensics Concepts and Approaches, B. Ravi Kumar Jain/ICFAI, University Press
3. Introduction to data communication and networking, Behrouz Forouzan, TMH

List of Suggested titles of Experiments (If Any):

1. Study about different network topology.
2. Study about different networking commands.
3. Study about firewall of different operating system.
4. Study about different cyber threats in Internet.
5. Study of tools used to detect the cyber threats in computers.
6. Using Wireshark, create a Filter to capture only FTP traffic.
7. Using wireshark, identify the version of SSL protocol used (SSLv1, SSLv2, SSLv3, TLSv1, TLSv2, etc) in any HTTPS web portal of your choice. You may need to login to get this information.
8. Carry out a port scanning on an internal lab machine using nmap.
9. Demonstration of sql injection.
10. A recent case study on cyber crime.

E-Resources (If any):

1. nptel.ac.in
2. <http://cyberlawsindia.net/>
3. <http://meity.gov.in/content/cyber-laws>