CYBER SECURITY

Course Code	23CS4601B	Year	III	Semester	II
Course Category	Professional Elective	Branch	CSE	Course Type	Theory
Credits	3	L – T – P	3-0-0	Prerequisites	Operating Systems, Computer Networks
Continuous Evaluation:	30	Semester End Evaluation:	70	Total Marks:	100

Course Outcomes		
Upon successful completion of the course, the student will be able to:		
CO1	Understand the basic concepts of cybercrime and cyber forensics.	L2
CO2	Apply various methods and tools to identify various cybercrimes.	L3
CO3	Apply the processes of cyber forensics in collecting, preserving, and preparing of digital evidence for analysis and investigations.	L3
CO4	Apply the legal perspectives of cybercrime in Indian IT Act.	L3

Syllabus

Unit No.	CONTENTS	Mapped CO
I	**Introduction to Cybercrime:** Introduction, Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Cyber criminals, Classifications of Cybercrime, Cyberstalking, Cybercafe and Cybercrimes, Botnets. Attack Vector, Proliferation of Mobile and Wireless Devices, Security Challenges Posed by Mobile Devices, Attacks on Mobile/Cell Phones.	CO1,CO2
II	**Tools and Methods :** Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggersand Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks, Identity Theft (ID Theft).	CO1,CO2

III	**Cyber Crime Investigation:** Introduction, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking	**CO1,CO3**
IV	**Computer Forensics and Investigations:** Understanding Computer Forensics, Preparing for Computer Investigations. Current Computer Forensics Tools: Evaluating Computer Forensics Tools, Computer Forensics Software Tools, Computer Forensics Hardware Tools, Validating andTesting Forensics Software, Graphics and Network Forensics, E-mail Investigations, Cell Phone and Mobile Device Forensics.	**CO1,CO3**
V	**Cyber Crime Legal Perspectives:** Introduction, Cybercrime and the Legal Landscape around the World, 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, Amendments to the Indian IT Act, Cybercrime and Punishment, Cyberlaw, Technology and Students: Indian Scenario	**CO1, CO4**

Learning Resources
Text Books
1. Sunit Belapure Nina Godbole "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", WILEY, 2011. 2. Nelson Phillips and Enfinger Steuart, "Computer Forensics and Investigations", Cengage Learning, New Delhi, 2009.
Reference Books
1. Michael T. Simpson, Kent Backman and James E. Corley, "Hands on Ethical Hacking and Network Defence", Cengage, 2019. 2. Computer Forensics, Computer Crime Investigation by John R. Vacca, Firewall Media, New Delhi. 3. Alfred Basta, Nadine Basta,Mary Brown and Ravinder Kumar "Cyber Security and Cyber Laws" , Cengage,2018.
E-Resources & other digital material
1. CERT-In Guidelines- http://www.cert-in.org.in/ 2. https://www.coursera.org/learn/introduction-cybersecurity-cyber-attacks [Online Course] 3. https://computersecurity.stanford.edu/free-online-videos [Free Online Videos] 4. Nickolai Zeldovich. 6.858 Computer Systems Security. Fall 2014. Massachusetts Institute of Technology: MIT OpenCourseWare, https://ocw.mit.edu License: Creative Commons BY-NC-SA.