

GANPAT UNIVERSITY									
FACULTY OF ENGINEERING & TECHNOLOGY									
Programme	Bachelor of Technology				Branch/Spec.	Computer Science & Engineering (CS)			
Semester	VI				Version	1.0.0.0			
Effective from Academic Year	2020-21				Effective for the batch Admitted in	June 2018			
Subject code	2CSE604		Subject Name	Cyber Crimes and Law					
Teaching scheme					Examination scheme (Marks)				
(Per week)	Lecture (DT)		Practical (Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	3	0	0	0	3	Theory	40	60	100
Hours	3	0	0	0	3	Practical	00	00	00
Pre-requisites:									
None									
Learning Outcome:									
After successful completion of this course, student will be able to									
<ul style="list-style-type: none"> <li>● Understand and describe the major types of cybercrime</li> <li>● Identify cybercrime vulnerabilities and exploitations of the Internet.</li> <li>● Understand the law with regards to the investigation and prosecution of cyber criminals.</li> <li>● Apply appropriate law enforcement strategies to both, prevent and control cybercrime.</li> </ul>									
Theory syllabus									
Unit	Content								Hrs
1	<b>Cyber Crime:</b> Definition and Origin of the Word, Cyber Crime and Information Security, who are Cyber Criminals, Classification of Cybercrimes, E-mail Spoofing, Spamming, 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								7
2	<b>Cyber Offenses:</b> 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								8
4	<b>Tools and Methods used in Cybercrime:</b> Proxy server and Anonymizers, phishing: How Phishing works? How password cracking works? Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Dos and DDOS Attacks, SQL Injection, Buffer Overflow, An Attacks on Wireless Networks								8
5	<b>Phishing and Identity Theft:</b> Phishing: Methods of Phishing, Phishing Techniques, Types of Phishing Scams, Phishing countermeasures, Identity theft, Types and Techniques of identity thefts and its counter measures								7
6	<b>IT ACT, Offenses and Penalties</b>								7

	Offences under the Information and Technology Act 2000 - Penalty and adjudication - Punishments for contraventions under the Information Technology Act 2000 (Case Laws, Rules and recent judicial pronouncements to be discussed) - Limitations of Cyber Law	
7	<b>Cybercrimes and Cyber security: The legal perspectives</b> Cybercrimes and the legal Landscape around the world, why do we need cyber laws: The Indian context, The Indian IT ACT: Admissibility of Electronic records, Amendments made in Indian ITA 2000, Positive Aspects and weak areas of ITA 2000, Challenges to Indian law and cybercrime scenario in India, Digital signatures and the Indian ITA act, Cybercrime and punishment, Cyber law Technology and students: Indian Scenario	8
<b>Suggested Practical content</b>		
● Case studies for cybercrime and implications through cyber laws.		
<b>Text/Reference Books</b>		
1	Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives By Nina Godbole, Sunit Belapur, Wiley	
2	Understanding Cybercrime: Phenomena, and Legal Challenges Response, ITU 2012	

<b>Course Outcomes:</b>												
COs												
CO1	Understand and describe the major types of cybercrime											
CO2	Identify cybercrime vulnerabilities and exploitations of the Internet											
CO3	Understand the law with regards to the investigation and prosecution of cyber criminals											
CO4	Apply appropriate law enforcement strategies to both, prevent and control cybercrime.											
<b>Mapping of CO and PO:</b>												
COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	0	0	3	0	0	0	2	0	0	2
CO2	3	3	3	0	3	0	0	0	0	0	0	1
CO3	3	2	0	0	2	0	0	0	0	0	2	0
CO4	3	2	2	0	3	0	0	0	0	0	2	0