Program Name			Semester		V
Course Title	**Cyber Security(Theory)**				
Course Code:	**SEC-5**		No. of Credits		**03**
Contact hours	**30Hrs**		Duration of SEA/Exam		**01hrs**
Formative Assessment Marks		**25**	Summative Assessment Marks		**25**

Course Outcomes(COs): After the successful completion of the course, the student will be able to:	
CO1	After completion of this course, students would be able to understand the concept of Cyber security and issues and challenges associated with it.
CO2	Students, at the end of this course, should be able to understand the cyber crimes, their nature, legal remedies and as to how report the crimes through available platforms and procedures.
CO3	On completion of this course, students should be able to appreciate various privacy and security concerns on online Social media and understand the reporting procedure of inappropriate content, underlying legal aspects and best practices for the use of Social media platforms.

Contents	**30Hrs**
Module-I. Introduction to Cyber security: Defining Cyberspace and Overview of Computer and Web-technology, Architecture of cyberspace, Communication and web technology, Internet, World wide web, Advent of internet, Internet infrastructure for data transfer and governance, Internet society, Regulation of cyberspace, Concept ofcyber security, Issues and challenges of cyber security.	10
Module-II . Cyber crime and Cyber law:Classification of cyber crimes, Common cyber crimes- cyber crime targeting computers and mobiles, cyber crime against women and children, financial frauds, social engineering attacks, malware and ransomware attacks, zero day and zero click attacks, Cybercriminals modus-operandi, Reporting of cyber crimes, Remedial and mitigation measures, Legal perspective of cyber crime, IT Act 2000 and its amendments, Cyber crime and offences, Organisations dealing with Cyber crime and Cyber security in India, Case studies.	10
Module III. Social Media Overview and Security: Introduction to Social networks. Types of Social media, Social media platforms, Social media monitoring, Hashtag, Viral content, Social media marketing, Social media privacy, Challenges, opportunities and pitfalls in online social network, Security issues related to social media, Flagging and reporting of inappropriate content, Laws regarding posting of inappropriate content, Best practices for the use of Social media, Case studies.	10

Course Articulation Matrix: Mapping of Course Outcomes (COs) with Program Outcomes

Course Out comes(COs) /Program Outcomes (POs)	**Program Outcomes (POs)**														
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Quickly understand the given problem and come up with the correct answer															
Identify, construct and compute numerical situations by work with numbers															

Conceive and develop a methodology for analyzing data and solving a problem.														
Define, modify and apply critical thinking to real time situations.														

Pedagogy: Problem Solving

Formative Assessment for Theory	
Assessment Occasion/type	**Marks**
Internal Test1	30%
Assignment/Surprise Test	20%
Total	**25Marks**
Formative Assessment as per guidelines.	

Text/References	
1	Cyber Crime Impact in the New Millennium, by R. C Mishra , Auther Press. Edition 2010
2	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011)
3	Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)
4	Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
5	Fundamentals of Network Security by E. Maiwald, McGraw Hill.
6	Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.