INSTITUTE	**FACULTY OF ENGINEERING AND TECHNOLOGY**
PROGRAM	**BACHELOR OF TECHNOLOGY (COMPUTER SCIENCE AND ENGINEERING -CYBER SECURITY)**
SEMESTER	**1**
COURSE TITLE	**CYBER SPACE & IT'S SECURITY**
COURSE CODE	**01CC0101**
COURSE CREDITS	**3**

Objective:

1 Students are expected to learn basics of Cyber Security fundamentals which will help them to know the importance of cyber space and cyber security concepts in day-to-day life. The course discusses various concepts about what, why, and how to the components are aligned in cyber world. Topics include fundamentals of cyber security, social media security, e-commerce security, cyber crime and cyber law.

Course Outcomes: After completion of this course, student will be able to:

1 Define key knowledge terminologies areas of cyber space & cyber security

2 Identify and explain measures for self-cyber-protection as well as societal cyber-protection.

3 Apply their knowledge to scenarios to reflect technology's latest capabilities and trends on cyber crime and cyber security

4 Analyze and evaluate the digital payment system security and remedial measures against digital payment frauds.

5 Analyze and evaluate existing legal framework and laws on cy

Pre-requisite of course:NA

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
3	0	0	50	30	20	0	0

Contents : Unit	Topics	Contact Hours
1	**Fundamentals of Cyber Space** 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 cyber space	7

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
2	**Cyber Crime** Concept of cyber security, Issues and challenges of cyber security. Introduction to Cybercrimes, Types of Crimes, Planning of Cybercrime, Cyber Crime against Individuals, Crime against Society, Crime against Organization, Introduction to hacking, types of hackers, White hat hacker, Black hat hacker, grey hat hacker, Hacking Privacy, How can we prevent against Hack, Viruses and Worms ,Phishing and Identify theft.	9
3	**E-Commerce and Digital Payments** Commerce threats, E-Commerce security best practices, Introduction to digital payments, Components of digital payment and stake holders, Modes of digital payments- Banking Cards, Unified Payment Interface (UPI), e-Wallets, Unstructured Supplementary Service Data (USSD), Aadhar enabled payments, Digital payments related common frauds and preventive measures, RBI guidelines on digital payments and customer protection in unauthorized banking transactions, Relevant provisions of payment settlement Act,2007	10
4	**Social Media Overview and Security** Introduction to Social networks. Types of Social media, Social media platforms, Social media monitoring, Hashtag, 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	9
5	**Cyber law** Introduction, importance of cyber law in human life, reporting of cyber crimes, Remedial and mitigation measures, Legal perspective of cyber crime, IT Act 2000 and its amendments, Cyber crime and offences, organizations dealing with Cyber crime and , Cyber security in India, Case studies.	7
Total Hours		**42**

Textbook :

1 Cyber Crime Impact in the New Millennium, R. C Mishra , Auther Press, 2010

References:

1 Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives , Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives , Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd, 2011

2 Security in the Digital Age: Social Media Security Threats and Vulnerabilities, Security in the Digital Age: Social Media Security Threats and Vulnerabilities, Henry A. Oliver, Pearson , 2015

References:

3 ELECTRONIC COMMERCE: FROM VISION TO FULFILLMENT, ELECTRONIC COMMERCE: FROM VISION TO FULFILLMENT, AWAD, ELIAS M., Prentice Hall of India Pvt Ltd, 2002

4 Cyber Laws: Intellectual Property & E-Commerce Security , Cyber Laws: Intellectual Property & E-Commerce Security , Krishna Kumar, Dominant Publishers & Distributors, 2011

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery and evaluation

Remember / Knowledge	Understand	Apply	Analyze	Evaluate	Higher order Thinking / Creative
25.00	25.00	15.00	20.00	15.00	0.00

Instructional Method:

1 a. The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

2 b. The internal evaluation will be done on the basis of continuous evaluation of students in the class-room.

3 c. Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory

Supplementary Resources:

1 1. https://onlinecourses.nptel.ac.in/noc23_cs127/preview

2 2. https://onlinecourses.swayam2.ac.in/nou19_cs08/preview

3 3. https://www.coursera.org/learn/cyber-security-fundamentals

4 4. https://www.netacad.com/courses/cybersecurity/introduction-cybersecurity

5 5. https://infyspringboard.onwingspan.com/web/en/app/toc/lex_3388902307073574000_shared/overview

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)