COURSE TITLE	**FUNDAMENTAL OF CYBER SECURITY**
COURSE CODE	**01CC0102**
COURSE CREDITS	**3**

Objective:

1 Students are expected to learn essentials of Cyber Security which will help them to know about the importance of data privacy and security concepts in day-to-day life. This course discusses various concepts about data privacy, security essentials, attacks and vulnerabilities identifications and understanding of hacking and cracking. Topics include digital security, data privacy in cyber space and organizational data protection.

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

1 Understand the importance of privacy for the personal, organizational and cyber data
2 Differentiate between threat, risk, attack and vulnerability.
3 Analyze and evaluate the importance of data, its privacy and security
4 Apply the protection measures to digital devices using latest tools and technologies
5 Evaluate Security Model of any organization

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	**Overview of cyber security** Cyber security increasing threat landscape, Cyber security terminologies- Cyberspace, attack, attack vector, attack surface, threat, risk, vulnerability, exploit, exploitation, hacker., Non-state actors, Cyber terrorism, Protection of end user machine, Critical IT and National Critical Infrastructure, Cyber warfare, Case Studies.	7
2	**Data and Data Privacy** Defining data, meta-data, big data, non-personal data, Data protection, Data privacy and data security, Personal Data Protection Bill and its compliance, Data protection principles, Big data security issues and challenges, Data protection regulations of other countries, General Data Protection Regulations (GDPR), 2016 Personal Information Protection and Electronic Documents Act (PIPEDA), Social media- data privacy and security issues	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
3	**Digital Security** digital security, protecting personal computers and devices, protecting devices from Virus, warms and Malware, Identity, Authentication and Authorization, need for strong credentials, keeping credentials secure, protecting servers using physical and logical security, World Wide Web (www), the Internet and the HTTP protocol, security of browser to web server Interaction.	7
4	**Digital Devices Security, Tools and Technologies for Cyber Security** End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third party software, Device security policy, Cyber Security best practices, Significance of host firewall and Ant-virus, Management of host firewall and Anti-virus, Wi-Fi security, Configuration of basic security policy and permissions.	7
5	**Privacy in Cyber Space** Introduction to cyber-attacks, application security (design, development and testing), operations security, monitoring, identifying threats and remediating them, Principles of data security - Confidentiality, Integrity and Availability, Data Privacy, Data breaches, preventing attacks and breaches with security controls, Compliance standards, Computer Ethics	7
6	**Security Essentials in Organizations** Security Planning, Business Continuity Planning, Handling Incidents, Risk Analysis, Dealing with Disaster, Hackers VS Ethical Hackers, Types of Hackers, Role of Ethical Hackers in Organizational security, Ethical Hackers in Organizational security,, International Laws - Cyber crime , Cyber Warfare and Home Land Security	7
Total Hours		**42**

Textbook :

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

References:

1 Cyberspace and Cybersecurity, Cyberspace and Cybersecurity, George Kostopoulos, CRC Press, 2013

2 Cyber Security: Analytics, Technology and Automation edited, Cyber Security: Analytics, Technology and Automation edited, 3. Martti Lehto, Pekka Neittaanma¨ki, Springer International Publishing Switzerland , 2015

3 Computer Forensics and Investigations, Computer Forensics and Investigations, 4. Nelson Phillips and Eninger Steuart, Learning, New Delhi, 2009

4 Security in Computing, Security in Computing, 5. Charles P. Pleeger Shari Lawrence Pleeger Jonathan Margulies, Pearson Education , 2018

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					
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/cec20_cs15/preview
3. 3. https://www.coursera.org/learn/introduction-to-cybersecurity-essentials
4. 4. https://www.netacad.com/courses/cybersecurity/cybersecurity-essentials
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)