Subject Syllabus

- Fundamentals of Information Security

Course: B.Tech. in Cyber Security **Semester: 1**

Prerequisite:

- NA.

Rationale:

- **Cybersecurity is the practice of deploying people, policies, processes and technologies to protect organizations, their critical systems and sensitive information from digital attacks**.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
3	0	0	0	3	60	20	-	20	-	100

SEE - Semester End Examination, **CIA** - Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) , **T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction to Cyber security & Ethical Hacking:** · Need of Cybersecurity · CIA Triad · Security Architecture · Security Governance · Security Auditing · Regulations & Frameworks · Ethical Hacking · Types of Hackers · Phases of Ethical Hacking · Penetration Testing · Types of Penetration Testing	20	6
2	**Exploring Ethics as it Relates to Cybersecurity:** · Differentiate between ethics and laws. · Distinguish among types of ethical concerns. · Define cyberbullying. · Identify actions that constitute cyberbullying. · Identify possible warning signs of someone being cyberbullied. · Identify laws applicable to cybersecurity.	20	9
3	**Understanding Cyber Threats and Vulnerabilities:** · Differentiate between a cyber threat and a vulnerability. · Describe types of cyber threats. · Analyze types of current cyber threats. · Describe the concept of malware and the techniques to guard against it. · Identify the perpetrators of different types of malicious hacking. · Describe the characteristics of vulnerabilities. · Identify the prevention of and protection against cyber threats.	20	10
4	**IdAM (Identity and Access Management):** · Authentication and authorization · Authentication and authorization principles · Regulation of access · Access administration · IdAM · Password protection · Identity theft.	20	10
5	**E-Commerce, Digital payments, and its security** Overview of social media and its security, Cyber security of digital devices, Tools and technology for cyber security, Cyber security plan and crisis management, Risk-based assessment, audit and compliance Cyber security best practices and do's and don'ts, Platforms to report and combat cybercrime	20	10

Course Outcome

After Learning the Course, the students shall be able to:

1. Reasonable understanding of the fundamentals of the cybersecurity domain and related issues

2. Practical knowledge of various tools, processes and methods to ensure security of systems through a minimum of two hands-on assignments involving attack and protection in a virtual environment

3. An understanding of the inter-disciplinary nature of cybersecurity domain

4. Adequate level of cross-disciplinary knowledge of design, implementation, evaluation and testing of secure protocols, systems or applications

5. Basic knowledge to be able to build bug-free systems, dependable during malice or error