B. Tech (Program) Honors/Minor* in Cyber Security and Forensics
T. Y. B. Tech. Computer Engineering
Pattern 2022 Semester: VI
COM223021 Cyber Security and Privacy

Teaching Scheme:	Credit Scheme:	Examination Scheme:
Theory: 04 hrs/week	04	Continuous Comprehensive Evaluation: 20 Marks InSem Exam: 20 Marks EndSem Exam: 60 Marks

Course Objectives:
- To Understand the Basic Concepts of Cyber Security and Information Systems
- To Develop Skills in Intrusion Detection and Prevention
- To Learn to Implement and Evaluate Security Models
- To Explore Security Challenges in Emerging Technologies
- To Understand the Legal and Forensic Aspects of Cyber Security

Course Outcomes: On completion of the course, students will be able to–

	Course Outcomes	Bloom's Level
CO1	Understand Cyber Space and Security Concepts	2-Understand
CO2	Apply Intrusion Detection and User Authentication Techniques	3-Apply
CO3	Summarize Security Models and Techniques	2-Understand
CO4	Describe Emerging Security Domains	2-Understand
CO5	Illustrate Cyber Crime Investigation Methods and Legal Aspects	2-Understand

COURSE CONTENTS

Unit I	Foundations of Cyber Space and Security	(06 hrs)	CO1

Introduction to Cyber Space, Understanding Cyber Space, Components and Dynamics, Introduction to Information Systems, Basics of Information Systems, Role in Cyber Space, Need for Cyber Security, Importance and Relevance, Key Concepts and Terminology.
Introduction to Cyber Attacks, Types and Examples, Impact and Consequences, Classification of Cyber Attacks, Different Types of Attacks, Characteristics and Examples, Classification of Malware, Threats, Types of Malware Identification and Mitigation

Unit II	Intrusion and User Authentication	(08 hrs)	CO2

Vulnerability Assessment, Identifying and Assessing Vulnerabilities, Tools and Techniques
Intrusion Detection Systems, Types of IDS Implementation and Management Intrusion Prevention Systems Preventive Measures Best Practices ,Introduction to User Authentication Methods Passwords, Tokens, and Multifactor Authentication Biometric Authentication Methods Types of Biometrics Use Cases and Applications Biometric Systems Design and Implementation Advantages and Challenges

Unit III	Security Models and Techniques	(08hrs)	CO3

Different Security Models and Security Mechanisms Overview of Security Models Mechanisms and Protocols ,Information Security and Network Security, Core Principles and Practices, Network Security Measures,, Operating System Security, Securing OS Components, Vulnerabilities and Patches, Web Security Securing Web Applications, Common Threats and Solutions, Email Security Protecting Email Communication, Threats and Countermeasures, Mobile Device Security, Cloud Security, Mobile Security Practices, Securing Cloud Services

Unit IV	**Specialized Security Domains**	**(06hrs)**	**CO4**

IoT Security Challenges in IoT, Best Practices and Standards, Cyber Physical System Security, Risk Management, Social Media Security, Protecting Privacy and Data, Threats and Mitigation, Virtual Currency Understanding Crypto currencies, Security Concerns Blockchain Technology Fundamentals of Blockchain, Security Implications, Security Auditing Conducting Security Audits, Compliance and Standards

Unit V	**Cyber Crimes, Forensics, and Legal Aspects**	**(08hrs)**	**CO5**

Cyber Crimes, Overview of Cyber Crimes, Types and Examples Different Types of Cyber Crimes, Scams, and Frauds, Identification and Prevention Case Studies Analysis of Crimes Digital Forensics, History, Challenges, Evolution of Digital Forensics, Current Challenges, Branches of Digital Forensics, Digital Forensic Investigation Methods, Investigation Protocols, Evidence Collection, Reporting, Management of Evidence, Documentation and Reporting, Evidence Handling, Cyber Law-Basics, Introduction to Cyber Laws, Key Principles, Information Technology Act 2000,Overview and Provisions, Amendments to IT Act 2000

Text Books

1. William Stallings, “Cryptography and Network Security Principals and Practice”, Seventh edition, Pearson , ISBN : 978-1-292-15858 2.
2. William Stallings, Lawrie Brown, “Computer Security Principles and Practice”, 3rd_Edition, Pearson , ISBN : 978-0-13-3777392-7 3.
3. Nina Godbole, Sumit Belapure, “Cyber Security”, Wiley, ISBN: 978-81-265-2179-1

Reference Books

1. Atul Kahate, “Cryptography and Network Security”, 3e, McGraw Hill Education
2. V.K. Pachghare, “Cryptography and Information Security”, PHI Learning
3. Bernard Menezes, “Network Security and Cryptography”, Cengage Learning India, 2014, ISBN No.: 8131513491

Strength of CO-PO PSO Mapping														
	PO												PSO	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3	2	3	2	-	-	-	-	-	-	-	3	3	2
CO2	3	3	2	2	-	-	-	-	-	-	-	3	3	3
CO3	3	3	3	2	-	-	-	-	-	-	-	3	3	3
CO4	3	3	3	2	-	-	-	-	-	-	-	3	3	3
CO5	3	3	3	2	-	-	-	-	-	-	-	3	3	3
Average	3	3	2	2	-	-	-	-	-	-	-	3	3	3

Guidelines for Continuous Comprehensive Evaluation of Theory Course		
Sr. No.	**Components for Continuous Comprehensive Evaluation**	**Marks Allotted**
1	Quiz on Unit 1, Unit-2, Unit-4, (Quiz 15 marks each and will be converted to 15 Marks)	15
2	Theory assignment on Unit-3 and Unit 5	10
	Total	**20**