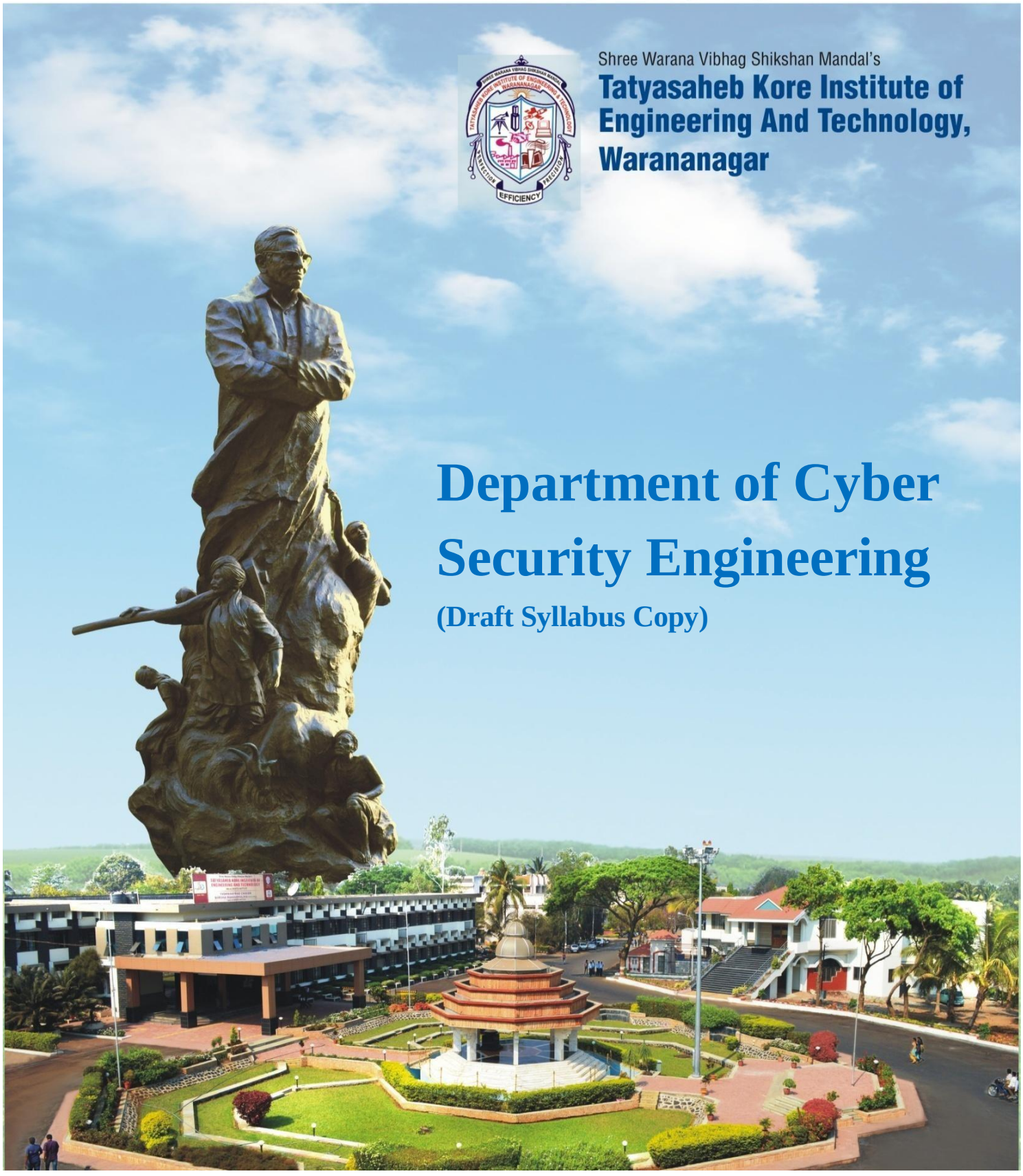
Shree Warana Vibhag Shikshan Mandal's
Tatyasaheb Kore Institute of Engineering And Technology, Warananagar
Department of Cyber Security Engineering
(Draft Syllabus Copy)

Department of Cyber Security Engineering

Vision

To become a center of excellence in the field of Cyber Security and to develop ethical cyber security professionals.

Mission

- To develop engineering graduates with high degree of processional excellence
- To excel in academics and research through contemporary and real world problems
- To enhance graduate employability through work based learning in social entrepreneurship
- To encourage industrial and nationally recognized institutes collaboration

Program Educational Objectives (PEOs)

Graduates will be,

- Apply core knowledge of cyber security and modern technologies to design, develop, and manage secure computing systems that address real-world challenges
- Pursue higher education, research, or entrepreneurial ventures with a strong foundation in cyber security principles and analytical skills.
- Demonstrate professionalism, effective communication, and ethical responsibility in addressing legal and societal aspects of cyber security.
- Collaborate effectively in multidisciplinary and multicultural teams to develop secure solutions for diverse domains.
- Exhibit leadership and contribute meaningfully to the protection of information infrastructure and national security.

Program Specific Outcomes (PEOs)

Graduate will be able to

- Graduates will be able to identify, analyze, and develop secure solutions to real-world problems by applying the principles of cyber security and secure software development lifecycle.
- Graduates will be capable of evaluating and implementing cyber security measures considering societal, ethical, and legal perspectives in the protection of digital assets.

Quality Policy

- To promote excellence in academic and training activities by inspiring students for becoming competent professionals to cater industrial and social needs.

Program Outcomes (POs)

The students after successfully completing this programme will have ability to:

- **PO1: Engineering Knowledge**:
  Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
- **PO2: Problem Analysis**:
  Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
- **PO3: Design/Development of Solutions**:
  Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
- **PO4: Conduct Investigations of Complex Problems**:
  Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
- **PO5: Modern Tool Usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
- **PO6: The Engineer and Society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice
- **PO7: Environment and Sustainability**:
  Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
- **PO8: Ethics**:
  Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
- **PO9: Individual and Team Work**:
  Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
- **PO10: Communication**:
  Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
- **PO11: Project Management and Finance**:
  Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
- **PO12: Life-long learning**:
  Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Department of Cyber Security Engineering

Abbreviations

Sr. No.	Acronym	Definition
1	ISE	In-Semester Examination
2	ISE-I	In-Semester Examination-I
3	ISE-II	In-Semester Examination-II
4	ESE	End Semester Examination
5	ISA	In-Semester Assessment (Term Work)
6	L	Lecture
7	T	Tutorial
8	P	Practical
9	CH	Contact Hours
10	C	Credit

Course Categories

Sr. No.	Acronym	Definition
1	BSC	Basic Science Course
2	HSC	Humanity Science Course
3	ESC	Engineering Science Course
4	PCC	Professional Core Course
5	OEC	Open Elective Course
6	MC	Mandatory Course
7	PEC	Professional Elective Course
8	PW	Project Work (Mini and Major Project)
9	II	Industrial Internship

Course/ Subject Code

C	S		3	0	1
Branch Code			Semester	Course Number	

Course Term work and POE Code

C	S		3	0	1	T / P / A
Branch Code			Semester	Course Number		T- Term work P- POE A- Audit Course

Second Year B. Tech.

in

Cyber Security Engineering

Syllabus Structure under Autonomous Status of TKIET, Warananagar

Semester-IV

(To be implemented from Academic Year 2025 - 26)

Credit Scheme

Semester-IV

(To be implemented from Academic Year 2025 - 26)

Credit Scheme

Sr. No	Category	Sub-Category	Course Code	Course Title	Teaching Scheme					Examination & Evaluation Scheme			
					L	T	P	C	CH	Component	Marks	Min for Passing	
1	Program Core Courses	PCC	25UG-PCC-CS401	Malware Fundamentals	3	--	--	3	3	ISE	40	16	40
										ESE	60	24	
2		PCC	25UG-PCC-CS402	Operating System	2	--	--	2	2	ISE	40	16	40
										ESE	60	24	
3		PCC	25UG-PCC-CS403	Web Designing	3	--	--	3	3	ISE	40	16	40
										ESE	60	24	
4		PCC	25UG-PCC-CS404	Cyber Ethics & Law	2	--	--	2	2	ISE	40	16	40
										ESE	60	24	
5	Multi-disciplinary Courses	MDM-2	25UG-MDM2-CS405	Malware Fundamentals	1	--	--	1	1	ISA (TW)	50	20	20
6		OE-1	25UG-OE1-CS406	Internet of Thing's	1	--	--	1	2	ISE	40	16	40
										ESE	60	24	
7	Skill Course	Vocational & Skill Enhancement Course (VSEC)	25UG-VSEC-CS407P	Python Programming	2	--	2	3	3	ISA	25	10	30
										ESE (POE)	50	20	
8	Humanities Social Science and Management	Ability Enhancement Course	25UG-AEC-CS408	Modern Indian Languages: Hindi	1	--	--	1	1	ISA (TW)	25	10	10
9		Entrepreneurship/ Economics/ Mgmt. Course	25UG-EEC2-CS409	Introduction to Cyber Security & Innovation	2	--	--	2	2	ISA (TW)	25	10	10
10		Value Education Course	25UG-VEC2-CS410	Cyber Ethics and Social Responsibility	1	--	--	1	1	ISA (TW)	25	10	10
11	Program Core Courses	PCC	25UG-PCC-CS401P	Malware Fundamentals Lab	--	--	2	1	2	ESE (POE)	50	20	20
12		PCC	25UG-PCC-CS403P	Web Designing Lab		--	2	1	2	ESE (POE)	50	20	20
					18	**--**	**6**	**21**	**24**	**--**	**800**	**320**	**320**

Second Year B. Tech. (Computer Science & Engineering)

Semester-IV

(To be implemented from 2025 - 26)

Credit Scheme

Department of Cyber Security Engineering

Guidelines for Course conduction and Evaluation in S.Y.B.Tech.(CS) Sem- III & Sem IV

1. A Moodle course structure is created for each course in the curriculum.
2. All the course teachers will upload course material, activities and assignments on moodle
3. All the students will be given a separate login credential on Moodle to access the contents in it.
4. The term work (ISA) will be assessed and evaluated as per the criteria defined in course contents.
5. ISE – I & ISE – II will of 40 Marks each: Average of Two ISEs will be considered to qualify.
6. **Minimum marks required to qualify for ISE : 16 out of 40 marks**
7. **Minimum marks required to qualify for TW: 10 out of 25 marks**
8. **Minimum marks required to qualify for TW: 20 out of 50 marks**
9. Completions of Audit Course activities are mandatory.

End Semester Examination (ESE- Theory):

1.	It will be conducted for 60 marks having 2 hours duration.
2.	Each Topic should have equal weightage.
4.	Theory Paper should contain the Theoretical as well as analytical questions.
5.	Minimum passing marks to be scored in ESE-T: 24 out of 60 marks

Second Year B. Tech. in

Cyber Security Engineering

Fourth (IV) Semester Detailed Syllabus

Second Year B. Tech(CS) (Semester – III)
25UG-PCC-CS401: Malware Fundamentals

Teaching Scheme	**Credits :** 03	**Examination Scheme**
Lectures: 03 Hrs / Week		**ESE:** 60 Marks **ISE:** 40 Marks

Course Description:

This course provides a foundational understanding of malware, its various forms, and how it affects computing environments. Students will explore the evolution, classification, and internal mechanisms of malware, including viruses, worms, trojans, ransomware, rootkits, and spyware.

Prerequisites:	1. Basic Operating System

Course Objectives:

1. Understand the fundamental concepts, characteristics, and classifications of malware.
2. Analyse the techniques used in the creation, obfuscation, and propagation of malware.
3. Identify and explain the functionality of various types of malware including viruses, worms, trojans, ransomware, and rootkits.
4. Apply both static and dynamic analysis methods to study and interpret malware behaviour.

Course Outcomes:

COs	**At the end of successful completion of the course the student will be able to**	**Blooms Taxonomy**
CO1	Understand the fundamental types, nature, and behaviour of malware	**Understand**
CO2	Apply static and dynamic analysis to detect malware activity	**Apply**
CO3	Analyse malware using reverse engineering techniques	**Analyze**

Course Contents

Unit-I	**Introduction to Malware**	**06 Hours**

Definition and classification of malware, Types of malware: Virus, Worms, Trojans, Ransomware, Rootkits, Adware, Spyware, Lifecycle of malware, Modes of malware propagation and activation, Recent malware trends

Unit-II	**Malware Analysis Techniques**	**08 Hours**

Static vs. dynamic malware analysis, Basic static analysis: File format, PE headers, strings, Basic dynamic analysis: Sandboxing, monitoring tools (Process Monitor, Wireshark)Behavioural and code analysis, Tools for malware analysis

Unit-III	**Malware Detection and Prevention**	**07 Hours**

Signature-based detection, Heuristic and behaviour-based detection, Machine learning approaches in malware detection, Memory forensics and endpoint protection tools, Antivirus and anti-malware software architecture

Unit-IV	Reverse Engineering of Malware	07 Hours
Introduction to reverse engineering, Disassemblers and debuggers: IDA Pro, Ghidra, OllyDbg, Understanding malware obfuscation and packing, Anti-reverse engineering techniques used by malware, Case study: Reverse engineering a known malware sample		
Unit-V	**Mobile and IoT Malware**	**06 Hours**
Introduction to mobile malware, Android and iOS malware architecture, IoT vulnerabilities and attack surfaces, Common malware in mobile and IoT environments, Mitigation and security practices for mobile/IoT devices		
Unit-VI	**Legal, Ethical and Defensive Strategies**	**06 Hours**
Ethical considerations in malware analysis, Cyber laws pertaining to malware creation and distribution, Creating secure environments for malware testing, Incident response to malware outbreaks, Best practices in malware defence and user awareness		

Course delivery methods	Assessment methods
1. Black Board Teaching 2. Power Point Presentation	1. Internal Assessment 2. Experiments 3. Quiz

Text Book:

1. Michael Sikorski, Andrew Honig, 'Practical Malware Analysis', No Starch Press
2. Mark Stamp, 'Information Security: Principles and Practice', Wiley

Reference Books:

1. Peter Szor, 'The Art of Computer Virus Research and Defense', Addison-Wesley
2. Chris Sanders, Jason Smith, 'Practical Packet Analysis', No Starch Press
3. SANS Reading Room – Malware Research Papers

CO-PO Mapping:

PO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	2	1	--	--	--	--	--	1	--	2
CO2	3	3	1	1	--	--	--	--	--	1	--	2
CO3	3	2	3	2	--	--	--	1	--	1	2	2

1-Low, 2-Medium, 3-High

----------END----------

Second Year B. Tech(CS) (Semester – III)
25UG-PCC-CS402: Operating System

Teaching Scheme	Credits:02	Examination Scheme
Lectures: 02 Hrs / Week		**ESE:** 60 Marks **ISE:** 40 Marks

Course Description:

This course is introduced at second year level to get the students familiar with the basic concepts of computer operating systems.

Prerequisites:	Basic Knowledge of Computer.

Course Objectives:

1. Make students understand basic concepts of operating system.
2. Understand what a process is and how processes are synchronized and scheduled.
3. Understand different approaches to memory management and I/O Management.

Course Outcomes:

COs	At the end of successful completion of the course the student will be able to	Blooms Taxonomy
CO1	Learn basic concepts of Operating Systems its types & services.	Remember
CO2	Describe various features of process and operation management	Understand
CO3	Present process synchronization and critical section problem with its solutions	Understand
CO4	Illustrate the working of different scheduling schemes and basics of deadlock with their possible solutions	Apply
CO5	Understand various memory management strategies like paging, swapping, and virtual memory management	Understand

Course Contents

Unit-I	Introduction, Overview and Structure of Operating Systems	06 Hours

Overview of Operating Systems, operations of an operating system, OS interaction with computers and user programs, Classes of an OS: Batch Processing, Multiprogramming, Time sharing system, Real-time OS, Distributed OS ,Operating System with Monolithic Structures ,Kernel based OS, Micro-kernel bases OS

Unit-II	Process Management	08 Hours

Process and Program, Implementing Process: Process state and state transition, Process context and process control block, Context save, scheduling and dispatching, event handling, sharing, communication and synchronization, Introduction to threads

Unit-III	Process Synchronization	07 Hours

What is process Synchronization, Race Condition, The Critical section problem, synchronization approaches: looping Vs blocking, H/W support for process synchronization, Classic process synchronization problems: Producer-consumer , Readers and writers, dining Philosophers, Semaphore

Unit-IV	Scheduling	07 Hours

Terminologies and concepts, Non- Pre-emptive scheduling: FCFS, SRN, HRN Pre-emptive scheduling: Round Robin, LCM, STG, Scheduling in practice: Long, medium and short term scheduler

Unit-V	Deadlock	06 Hours

What is deadlock, Deadlock in resource allocation, handling deadlocks, Deadlock detection and resolution, Deadlock prevention, Deadlock avoidance.		
Unit-VI	**Memory Management**	**06 Hours**
Memory allocation to a process: Stack and Heap, Memory allocation Model Heap Management: Reuse of memory, Contiguous memory, Non- Contiguous memory Paging, Segmentation. Virtual Memory Basics, Page replacement Policies		

Course delivery methods	Assessment methods
1. Black Board Teaching 2. Power Point Presentation	1. Internal Assessment 2. Experiments 3. Quiz

Text Book:

1. Operating Systems- A Concept-Based Approach Dhananjay M. Dhamdhere (MGH International) 3rd Edition 2006

Reference Books:

1. Operating Systems –Concepts and Design, Milan Milenkovic TATA-McGraw Hill, 9th Edition
2. Operating Systems: Internals and Design Principles William Stallings AT&T Bell Labs, 8th Edition

CO-PO Mapping:

PO / CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	1	-	-	-	-	-	-	-	-	-	-	1
CO2	1	-	-	-	-	-	-	-	-	-	-	1
CO3	1	-	2	3	-	-	-	-	-	-	-	1
CO4	1	2	1	1	-	-	-	-	-	-	-	1
CO5	1	1	1	-	-	-	-	-	-	-	-	1

1-Low, 2-Medium, 3-High

----------END----------

Second Year B. Tech(CS) (Semester – III)

25UG-PCC-CS403 : Web Designing

Teaching Scheme	**Credits:**03	**Examination Scheme**
Lectures: 03 Hrs / Week		**ESE:** 60 Marks
		ISE: 40 Marks

Course Description:

This course provides foundational knowledge and practical skills in designing and developing responsive and accessible websites. Students will learn HTML, CSS, JavaScript, and essential concepts of UI/UX, with an emphasis on secure web design practices aligned with modern standards.

Prerequisites:	1. Basic Programming Concepts (C/C++)

Course Objectives:

1. Understand the structure and working of the web.
2. Learn to design static and dynamic web pages using HTML, CSS, and JavaScript.
3. Gain proficiency in responsive design and UI/UX principles.
4. Learn and apply secure coding practices in web design.
5. Use web development tools and frameworks effectively.

Course Outcomes:

COs	**At the end of successful completion of the course the student will be able to**	**Blooms Taxonomy**
CO1	Describe the structure of the web and use HTML to create basic web pages.	**Understand**
CO2	Apply CSS to style HTML pages responsively.	**Apply**
CO3	Use JavaScript to add interactivity and validate inputs securely.	**Analyze**
CO4	Design user-friendly and secure websites incorporating best UI/UX practices.	**Apply**
CO5	Deploy and manage websites using version control and hosting platforms.	**Apply**

Course Contents

Unit-I	**Introduction to Web & Internet Basics**	**04 Hours**

Evolution of Web Technologies (Web 1.0 to 5.0), Internet, WWW, URLs, HTTP/HTTPS, DNS, Web Servers, Domain Names, Hosting, Introduction to browsers and developer tools, Secure Web Browsing & Certificate Verification

Unit-II	**HTML5 - Structure and Semantics**	**08 Hours**

HTML Elements, Tags, Attributes, Forms, Input Types, HTML Tables, Lists, Multimedia: Audio, Video, Canvas, SVG, Semantic Elements: <article>, <section>, <nav>, etc., SEO Fundamentals and Accessibility Features

Unit-III	**CSS3 - Styling the Web**	**07 Hours**

Introduction to CSS and Selectors, Box Model, Positioning, Flexbox, Grid, Pseudo-classes & Pseudo-elements, Responsive Design: Media Queries, Styling Forms and Tables

Unit-IV	**JavaScript - Client-side Scripting**	**07 Hours**

Introduction to JavaScript syntax and data type, Functions, DOM Manipulation, Events Handling, Forms Validation, JavaScript Security Best Practices (XSS, Input Sanitization), Debugging with Browser Dev Tools

Unit-V	**Advanced Web Design Concepts**	**06 Hours**

UI/UX Principles and Design Thinking, Introduction to Bootstrap and Responsive Frameworks, CSS Animations & Transitions, Progressive Web Apps (PWA) Overview, Introduction to Git & GitHub for version control

Unit-VI	Secure Web Development & Deployment	06 Hours
OWASP Top 10 for Web Security, Input validation, session management, HTTPS, CSP, Cookies and Local Storage, Hosting Static Sites (GitHub Pages/Netlify), Basic Web Performance Optimization Techniques		

Course delivery methods	Assessment methods
1. Black Board Teaching 2. Power Point Presentation	1. Internal Assessment 2. Experiments 3. Quiz

Text Book:

1. Jon Duckett, HTML and CSS: Design and Build Websites, Wiley
2. Thomas Powell, JavaScript: The Complete Reference, McGraw-Hill

Reference Books:

1. Robin Nixon, Learning PHP, MySQL & JavaScript, O'Reilly
2. Ethan Marcotte, Responsive Web Design, A Book Apart
3. Feras A. Batarseh, Cybersecurity for Web Developers, CRC Press

CO-PO Mapping:

PO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	--	--	--	--	--	--	--	2	--	2
CO2	3	2	2	--	2	--	--	--	--	2	--	2
CO3	3	3	2	1	2	2	2	--	--	2	1	2
CO4	3	3	3	2	2	1	2	2	2	3	1	3
CO5	2	3	3	2	3	--	2	--	--	2	2	3

1-Low, 2-Medium, 3-High

----------END----------

Second Year B. Tech(CS) (Semester – III)

25UG-PCC-CS404: Cyber Ethics & Law

Teaching Scheme	**Credits :** 02	**Examination Scheme**
Lectures: 02 Hrs / Week		**ESE:** 60 Marks
		ISE: 40 Marks

Course Description:

This course explores the ethical, legal, and societal issues arising from the use of digital technology and the Internet. It examines how legal frameworks and ethical principles apply to cyber security, data privacy, intellectual property, cybercrimes, and the responsibilities of professionals in the cyber domain.

Prerequisites:	Basic understanding of Computers, Internet and Introduction to Cyber Security

Course Objectives:

1. Understand the fundamental principles of cyber ethics and professional responsibility in the digital world.
2. Explain key cyber laws, legal systems, and frameworks applicable to cybercrime and digital evidence.
3. Identify and analyze ethical dilemmas and legal challenges in areas such as privacy, surveillance, and digital forensics.
4. Evaluate the implications of cybercrime legislation at both national and international levels.

Course Outcomes:

COs	**At the end of successful completion of the course the student will be able to**	**Blooms Taxonomy**
CO1	Explain cyber laws and ethical challenges in the digital era	**Understand**
CO2	Analyze Indian IT laws and their enforcement in various cyber crime contexts.	**Analyze**
CO3	Evaluate privacy laws, data protection frameworks, and	**Evaluate**
CO4	Apply professional ethics in real-world cyber security scenarios	**Apply**

Course Contents

Unit-I	**Introduction to Cyber Law and Ethics**	**05 Hours**

Definition and importance of Cyber Law, Need for cyber laws in the digital era, Ethics in cyberspace: Importance, challenges, and global view, Understanding ethical hacking vs. malicious hacking, Case studies on cyber ethical dilemmas

Unit-II	**Legal Framework in India**	**05 Hours**

Overview of the Information Technology Act, 2000, Amendments to the IT Act and related cyber regulations, Legal recognition of electronic records and digital signatures, Cybercrime and legal consequences under IPC and IT Act, Authorities under the IT Act – CERT-IN, Adjudicating Officers, Cyber Appellate Tribunal

Unit-III	**Cyber Crimes and Legal Remedies**	**05 Hours**

Types of cyber crimes: Identity theft, financial fraud, cyber terrorism, cyberstalking, Investigation and enforcement procedures, Jurisdictional challenges and cross-border data issues, Cyber forensics and evidence collection, Real-life examples and court judgments

Unit-IV	**Privacy, Data Protection and Intellectual Property**	**08 Hours**

Understanding digital privacy and data protection laws, GDPR Overview and comparison with Indian framework, Personal Data Protection Bill (India) – Key aspects and provisions, Intellectual Property Rights (IPR) in digital space, Copyrights, Patents, Trademarks and software licensing issues

Unit-V	**Internet Governance and Global Perspectives**	**05 Hours**

Need and role of Internet Governance, ICANN, ITU, IGF and other international stakeholders, Cross-border cyber law enforcement issues, Safe harbor principles and intermediary liabilities, Digital sovereignty and cyber diplomacy		
Unit-VI	**Ethics for Cyber Security Professionals**	**08 Hours**
Professional conduct and responsibilities in cyber space, Ethical codes by IEEE, ACM, (ISC)², ISACA, Handling vulnerabilities and responsible disclosure, Case studies of ethical vs. unethical practices, Ethics in artificial intelligence and surveillance technologies		

Course Delivery Method	Course Assessment Method
1. Chalk and board 2. Presentation Slides 3. Pre recorded Video lectures	1. Internal assessment 2. Problem Solving 3. Topic wise Quizzes

Text Book:

1. Sunit Belapure and Nina Godbole, 'Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives', Wiley
2. Justice Yatindra Singh, 'Cyber Laws', Universal Law Publishing Co.

Reference Books:

1. Pavan Duggal, 'Cyber Law: The Indian Perspective', Saakshar Publications
2. Jonathan Rosenoer, 'CyberLaw: The Law of the Internet', Springer
3. Indian IT Act 2000 with Amendments (available online via Ministry of Electronics & IT)

CO-PO Mapping:

PO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	1	2	--	--	1	--	1	--	--	1	1
CO2	2	3	1	--	--	--	--	1	--	--	--	--
CO3	2	1	--	--	2	--	--	1	--	--	--	--
CO4	2	3	2	2	2	--	--	1	--	--	--	1

1-Low, 2-Medium, 3-High

----------**END**----------

Second Year B. Tech(CS) (Semester – III) 25UG-PCC-CS401P: Malware Fundamentals Lab		
Teaching Scheme Lectures: **Practical:** 02 Hrs / Week	**Credits :**01	**Examination Scheme** **ESE(POE):** 50 Marks

Experiment List:

Experiment No	Problem Statement	Blooms Taxonomy
Experiment No 1	Static analysis of a PE file using PEStudio	**Apply**
Experiment No 2	Using Process Monitor for dynamic behavior analysis	**Apply**
Experiment No 3	Packet capture and inspection of malware communication using Wireshark	**Apply**
Experiment No 4	Reverse engineering using Ghidra or IDA Free	**Apply**
Experiment No 5	Detecting malware using VirusTotal and YARA rules	**Apply**
Experiment No 6	Unpacking a simple packed malware sample	**Apply**
Experiment No 7	Monitoring registry/file system changes by malware	**Apply**
Experiment No 8	Simulating and analyzing a ransomware attack in a VM environment	**Apply**

----------**END**----------

Second Year B. Tech(CS) (Semester – III) 25UG-PCC-CS403P: Web Designing Lab		
Teaching Scheme Lectures: **Practical:** 02 Hrs / Week	**Credits :**01	**Examination Scheme** **ESE(POE):** 50 Marks

Experiment List:

Experiment No	Problem Statement	Blooms Taxonomy
Experiment No 1	Create a basic HTML page with headings, paragraphs, images, and links.	**Apply**
Experiment No 2	Design a feedback form using HTML5 form elements and validation.	**Apply**
Experiment No 3	Develop a web page using CSS Flexbox/Grid to layout a responsive design.	**Apply**
Experiment No 4	Apply transitions and animations in a CSS-based menu.	**Apply**
Experiment No 5	Use JavaScript to validate form inputs dynamically.	**Apply**
Experiment No 6	Create a responsive navigation bar using Bootstrap.	**Apply**
Experiment No 7	Build a photo gallery using JavaScript and CSS effects.	**Apply**
Experiment No 8	Implement local storage in a simple to-do web application.	**Apply**
Experiment No 9	Deploy a static website using GitHub Pages or Netlify.	**Apply**
Experiment No 10	Mini project: Design and host a secure, responsive multipage website (team-based).	**Apply**

----------END----------

Second Year B. Tech(CS) (Semester – III)

25UG-MDM2-CS405: Malware Fundamentals

Teaching Scheme	**Credits :**01	**Examination Scheme**
Lectures: 01 Hrs / Week		**ISA(TW):** 50 Marks

Course Description:

This course provides a foundational understanding of malware, its various forms, and how it affects computing environments. Students will explore the evolution, classification, and internal mechanisms of malware, including viruses, worms, trojans, ransomware, rootkits, and spyware.

Prerequisites:	1. Basic Operating Systems, Computer Networks, Introduction to Cyber Security.

Course Objectives:

1. Understand the fundamental concepts, characteristics, and classifications of malware.
2. Analyse the techniques used in the creation, obfuscation, and propagation of malware.
3. Identify and explain the functionality of various types of malware including viruses, worms, trojans, ransomware, and rootkits.
4. Apply both static and dynamic analysis methods to study and interpret malware behaviour.

Course Outcomes:

COs	**At the end of successful completion of the course the student will beable to**	**Blooms Taxonomy**
CO1	Understand the fundamental types, nature, and behavior of malwar	**Understand**
CO2	Apply static and dynamic analysis to detect malware activity	**Apply**
CO3	Analyze malware using reverse engineering techniques	**Analyze**

Course Contents

Unit-I	**Introduction to Malware**	**04 Hours**

Definition and classification of malware, Types of malware: Virus, Worms, Trojans, Ransomware, Rootkits, Adware, Spyware, Lifecycle of malware, Modes of malware propagation and activation, Recent malware trends

Unit-II	**Malware Analysis Techniques**	**08 Hours**

Static vs. dynamic malware analysis, Basic static analysis: File format, PE headers, strings, Basic dynamic analysis: Sandboxing, monitoring tools (Process Monitor, Wireshark)Behavioral and code analysis, Tools for malware analysis

Unit-III	**Malware Detection and Prevention**	**07 Hours**

Signature-based detection, Heuristic and behavior-based detection, Machine learning approaches in malware detection, Memory forensics and endpoint protection tools, Antivirus and anti-malware software architecture

Unit-IV	**Reverse Engineering of Malware**	**07 Hours**

Introduction to reverse engineering, Disassemblers and debuggers: IDA Pro, Ghidra, OllyDbg, Understanding malware obfuscation and packing, Anti-reverse engineering techniques used by malware, Case study: Reverse engineering a known malware sample

Unit-V	Mobile and IoT Malware	06 Hours
Introduction to mobile malware, Android and iOS malware architecture, IoT vulnerabilities and attack surfaces, Common malware in mobile and IoT environments, Mitigation and security practices for mobile/IoT devices		
Unit-VI	**Legal, Ethical and Defensive Strategies**	**06 Hours**
Ethical considerations in malware analysis,Cyber laws pertaining to malware creation and distribution, Creating secure environments for malware testing, Incident response to malware outbreaks, Best practices in malware defense and user awareness		

Course delivery methods	Assessment methods
1. Black Board Teaching 2. Power Point Presentation	1. Internal Assessment 2. Experiments 3. Quiz

Text Book:

1. Michael Sikorski, Andrew Honig, 'Practical Malware Analysis', No Starch Press
2. Mark Stamp, 'Information Security: Principles and Practice', Wiley

Reference Books:

1. Peter Szor, 'The Art of Computer Virus Research and Defense', Addison-Wesley
2. Chris Sanders, Jason Smith, 'Practical Packet Analysis', No Starch Press
3. SANS Reading Room – Malware Research Papers

CO-PO Mapping:

PO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	2	1	--	--	--	--	--	1	--	2
CO2	3	3	1	1	--	--	--	--	--	1	--	2
CO3	3	2	3	2	--	--	--	1	--	1	2	2

1-Low, 2-Medium, 3-High

----------END----------

Second Year B. Tech(CS) (Semester – III)

25UG-OE1-CS406: Internet of Things

Teaching Scheme	**Credits:**01	**Examination Scheme**
Lectures : 01 Hrs / Week		**ISE:** 40 Marks
		ESE: 60 Marks

Course Description:

This course provides an in-depth introduction to the Internet of Things (IoT), covering fundamental mechanisms, identification technologies, communication protocols, and practical applications, including hands-on experience with Raspberry Pi and various IoT systems.

Prerequisites:	**1.** Fundamentals of Computer Network and Internet

Course Objectives:

1. To understand core IoT concepts and frameworks.
2. To Provide knowledge on IoT mechanisms, including traffic characteristics, scalability, and security.
3. Understanding of RFID technology and its components in IoT systems.
4. Enable hands-on experience with IoT hardware and software, focusing on Raspberry Pi.
5. To apply IoT technologies in real-world scenarios like smart cities and home automation.

Course Outcomes:

COs	**At the end of successful completion of the course the student will be able to**	**Blooms Taxonomy**
CO1	To discuss IoT Concepts and Frameworks	**Understand**
CO2	To learn and implement RFID technology in various applications	**Remember**
CO3	To identify and describe the components of an RFID system	**Understand**
CO4	To write programs for basic applications	**Understand**
CO5	To state IoT technologies in various real-world applications	**Remember**

Course Contents

Unit-I	**Introduction**	**06 Hours**

IoT, Objects / Things, IoT definitions, IoT frame work, Identification technologies, Internet in IoTs.

Unit-II	**Fundamental of IoT mechanisms**	**06 Hours**

Identification of IoT objects and services, Traffic characteristics, scalability and interoperability, security and privacy, Communication capabilities, Mobility support and device power, Sensor technology, RFID technology and satellite technology.

Unit-III	**Radio Frequency Identification Technology**	**06 Hours**

RFID, IoT objects and services, principles of RFID, Components of an RFID system, RFID reader, Tags, middleware, Sensor nodes, connecting nodes, networking nodes.

Unit-IV	**IoT systems**	**07 Hours**

Hardware and Software: Introduction to Raspberry Pi, Familiar with Raspberry Pi hardware, study of I/O ports, Programming with Raspberry Pi: Study of operating system.

Unit-V	Communication Technologies	07 Hours
WPAN Technologies: Introduction to IEEE 802.15.4 standard, Bluetooth, Zigbee, IEEE 802.15.6; WBANS, NFC, WLAN, Cellular and mobile technologies		
Unit-VI	**IoT Application Examples**	**07 Hours**
Smart Metering, advanced metering infrastructure, e-health / Body Area Network, City Automation (Smart City), Automotive Application, Environmental Applications, Home Automation, Control Applications		

Course delivery methods	Assessment methods
1. Black Board Teaching 2. Power Point Presentation	1. Internal Assessment 2. Assignment 3. Quiz

Text Books

1. The Internet of Things-Connecting Objects to the Web, Hakima Chaouchi Wiley Publications 1st Edition 2010.
2. Building the Internet of Things, Daniel Minoli, Wiley Publications, 1st Edition-2013

Reference Books

1. Raspberry Pi for Dummies, Sean McManus, Mike Cook, Wiley (2 March 2023); Wiley India Pvt Ltd
2. Architecting the Internet of Things-Bernd Scholz, Reiter Springer 1st edition 2011

CO-PO Mapping:

PO / CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	1	2	1	2	2	1	1	1	1	1	3
CO2	3	2	2	3	3	1	1	1	1	1	1	2
CO3	3	3	2	2	3	1	1	1	1	1	1	2
CO4	3	3	3	3	3	1	1	1	2	2	2	3
CO5	3	2	3	3	3	3	3	2	3	3	3	3

1-Low, 2-Medium, 3-High

----------END----------

Second Year B. Tech(CS) (Semester – III)

25UG-VSEC-CS407: Python Programming

Teaching Scheme	**Credits:**02	**Examination Scheme**
Lectures : 02 Hrs / Week		**ISE:** 40 Marks **ESE:** 60 Marks

Course Description:

This course provides an introduction to Python Programming language. Students are introduced to key programming concepts like data structures, conditionals, loops, variables, and functions.

Prerequisites:	1. Computer Programming in C 2. Data Structure

Course Objectives:

1. To learn and understand programming paradigm and Python basics.
2. To learn and understand python looping, control statements and string manipulations.
3. To acquire Object Oriented Programming skills and concepts of file handling.

Course Outcomes:

COs	**At the end of successful completion of the course the student will be able to**	**Blooms Taxonomy**
CO1	To recall the concepts of Python Programming Language in Problem Solving scenario	**Remember**
CO2	Utilize of key concepts in the file handling, string handling, exception handling of strings and functions	**Apply**
CO3	To illustrate object-oriented concepts in various real time problems	**Apply**
CO4	To implement file handling and exception handling concepts for a given scenario	**Apply**
CO5	Plotting the data using appropriate Python visualization libraries/packages	**Apply**

Course Contents

Unit-I	**Basics of Python Programming**	**07 Hours**

Features of Python, History and Future of Python, Writing and executing Python program, Literal constants, variables and identifiers, Data Types, Input operation, Comments, Reserved words, Indentation, Operators and expressions Decision Control Systems: Selection/conditional branching Statements: if, if-else, nested if, if-elif-else statements. Basic loop Structures/Iterative statements: while loop, for loop, selecting appropriate loop. Nested loops, The break, continue, pass, else statement used with loops.

Unit-II	**Functions and Modules**	**06 Hours**

Definition, call, variable scope and lifetime, the return statement. Defining functions, Lambda or anonymous function, documentation string, good programming practices. Introduction to modules, Introduction to packages in Python, Introduction to standard library modules.

Unit-III	**Python Strings & Data Structures**	**06 Hours**

Python Strings: Concatenating, appending & multiplying strings, built in string functions, slicing, comparing strings Data Structures: Sequence, Lists, Tuples, Set, Dictionaries

Unit-IV	Classes and Objects	07 Hours
Creating and Using a Class, Working with Classes and Instances, Inheritance & Polymorphism.		
Unit-V	**Exception Handling & File Handling**	**07 Hours**
Exception Handling: Introduction to Errors & Exceptions, handling exceptions, multiple except blocks. File Handling: Introduction, File path, Types of files, Opening and Closing files, Reading and Writing files.		
Unit-VI	**Data Analysis & Visualization**	**07 Hours**
NumPy: Creating Arrays, Array indexing, Array Slicing & Built-in Functions Pandas: Series, Framework, Built-in Functions of pandas Matplotlib: Plotting, marker, labels, grid, scatter, bars, histograms, pie charts		

Course delivery methods	Assessment methods
1. Black Board Teaching 2. Power Point Presentation	1. Internal Assessment 2. Assignment 3. Quiz

Text Books

1. Python Programming Using Problem Solving Approach (for Unit 1,2,3,4),Reema Thareja Oxford University Press.-2017
2. Python Crash Course: A Hands-On Project-Based Introduction to Programming (for Unit 5,6)Eric Matthes No Starch Press-2019

Reference Books

1. Core Python Programming-R. Nageswara Rao, Dreamtech Press, 2nd (2017)
2. Learning Python, Romano Fabrizio Packt Publishing Limited,2nd Edition (2015)

Experiment List

Experiment No	Problem Statement	Blooms Taxonomy
Experiment No 1	[Basic] Handling of different data types and arithmetic operations	**Apply**
Experiment No 2	[Control Flow] Handling various loops, control statements	**Apply**
Experiment No 3	[Control Flow] Performing various operation on String (String Handling)	**Apply**
Experiment No 4	[Data Structure] Handling Python Data Structures	**Apply**
Experiment No 5	[File] Different File Handling Operations	**Apply**
Experiment No 6	[Functions] Concepts of function and its usage	**Apply**
Experiment No 7	[Object Oriented Programming] Concepts of constructor and Inheritance in Python	**Apply**
Experiment No 8	(a) To demonstrate working of classes and objects (b) To demonstrate constructors (c) To demonstrate class method and static method	**Apply**
Experiment No 9	Concept of polymorphism in python (method overloading and overriding)	**Apply**
Experiment No 10	Concepts of Data Analysis and Visualization	**Apply**

CO-PO Mapping:

PO / CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	-	1	-	-	-	-	-	-	-	-	2
CO2	3	3	1	2	2	-	-	-	-	-	1	2
CO3	3	2	2	3	3	1	-	-	1	-	1	2
CO4	3	2	3	1	1	2	1	-	2	1	2	2

1-Low, 2-Medium, 3-High

----------END----------

Second Year B. Tech(CS) (Semester – III)

□□□□□□ □□□□□□ □□□□

25UG-AEC1-CS408-1: Modern Indian Languages :- □□□□□□□□□□□ □□□□□

□□□□□□□□□□□□: २ तास / सप्ताह	□□□□□□□□ : 01	□□□□ □□□□□□□□□: □□ □□□

□□□□□:

"□□□□□□□□□□□ □□□□□" □□ □□□□ □□ □□□□□□ □□□□□□□ □□□□□□□□ □□ □□□□□□□ □□□□□ □□□□ □□□ □□□ □□□□□□□□ □□□□□□□□□□ □□□□□□□□□□ □□ □□□□□□□□□□ □□□ □□□□□□ □□ □□□□□□□ □□ □□□□□□□□□ □□ □□□□□□□ □□□ □□ □□□□□ □□□ □□□ □□□□□ □□□ □□□□□□□□□ □□□ □□□□□□□□□□□ □□□□□ □□ □□□□□ □□ □□□□ □□□□□□□□□□□ □□ □□□ □□ □□ □□□□ □□□ □□ □□□□ □□ □□□□□ □□ □□ □□□□ □□ □□□□□ □□□□□□□□ □□□ □□ □□□□ □□ □□□□□□□, □□□□□□□□□□ □□□□□□□□, □□□□□□, □□□□□□□□ □□□□ □□ □□□□□□□□ □□□□□□□□ □□ □□□□□□□□ □□ □□□□□ □□□□ □□□ □□|

□□□□□□□□:

1. □□□□□ □□ □□□□□□□□□□ □□□□ □□ □□□□□□ □□□□□
2. □□□□□□□□□ □□□□□□□ □□□ □□□□□ □□□□ □□ □□□□□□□□□ □□□□□
3. □□□□□ □□□ □□□□□ □□□□ □□ □□□□ □□□□□□ □□□□□
4. □□□□□□□□□□□ □□ □□□□□ □□□□ □□□□□□□ □□□□□
5. □□□□□□□□ □□ □□□□□□□ □□□ □□□□□ □□□□□□ □□ □□□□ □□□□□□ □□□□□.

□□□□□□:

□□□□□□□□ □□ □□□ □□□□□ □□ □□□□□ □□□□□□□□□□ □□□□□□□□□ □□ □□□□□□□ □□□□□

□	□□□□□ □□ □□□□□□□□□□ □□ □□□□□□□□□ □□□□ □□ □□□□□□ □□□□.

□	□□□□ □□□□□□□□□□ □□□ □□□□□ □□□ □□□□ □□ □□□□□□ □□□□□
□	□□□□ □□ □□□□□□□□ □□□ □□ □□□□□□□ □□□□□ □□□ □□□□□□ □□ □□□□□
□	□□□□□□□□□□□ □□ □□□□□□ □□ □□□□□□ □□ □□□□□□

□□□□ □□□□□ □□□□□□□□□□

□□□□ □	□□□□□□□□□□ □□□□□□□□	□□ घंट
□□□□□ □□ □□□ □□□□□ □□□□, □□□□□□□□□□□□□ □□□ □□□□, □□□□□□ □□ □□□ □□□□□□□□□ □□□□, □□□□□□□		
□□□□ □	□□□□□□	□□ घंट
□□□□□□ □□ □□□□□□□, □□□□□□ □□ □□□□□□, □□□□□□ □□ □□□□□□□□, □□□□□□□ □□ □□□		
□□□□ □	□□□□□□□□ □□□□	□□ घंटे
□□□□□□□□□□□□□ □□□□□□ □□ □□□□□□□□□ □□□□, □□□□□□□ □□□□□□ □□ □□□□□□□□□ □□□□, □□□□□□□□□□ □□□□□□□□ □□□□□□□□□ □□□□, □□□□□□□□□□□□ □□□□□□□□□ □□□□		
□□□□ □	□□□□□□□ □□□□□□□□	□□ घंटे
□□□□□□ □□ □□□□, □□□□□□□□ □□ □□□□, □□□□□□□ □□ □□□□, □□□□□□ □□ □□□□		

□□□□□□ □□□□□□□□□	
□	□□□□□ □□ □□□□ □□□□□□□- □□. □□□□. □□. □□□□, □□□□ □□□□□□□, □□□□□□□□.
□	□□□□□□□□□□□□- □□. □□□□□□ □□□□□□, □□□ □□□□□□□, □□□□□□.
□	□□□□□□□□□□□ □□□□□ □□□□□□□ □□□ □□□□□□□□- □□.

	□□□□□□□□ □□□□□□, □□□□□ □□□□□□□□, □□□□□□□
□	□□□□□□□□□□□□□□□ □□□□□□- □□. □□□□□ □□□□□□, □□□□□ □□□□□□□□, □□□□□□□

----------END----------

Second Year B. Tech(CS) (Semester – III)

25UG-EEC2-CS409: Introduction to Cyber Security & Innovation

Teaching Scheme	**Credits:**02	**Examination Scheme**
Lectures : 02 Hrs / Week		**ISA:** 25 Marks

Course Description:

To introduce students to the fundamentals of cybersecurity threats, tools, and frameworks.

Prerequisites:	1. Basic Computer Fundamentals 2. Introduction to Networking or Information Technology

Course Objectives:

1. To introduce students to the fundamentals of cybersecurity threats, tools, and frameworks.
2. To inspire innovation by connecting security challenges to entrepreneurial opportunities.
3. To develop an understanding of how emerging technologies affect cybersecurity.
4. To introduce design thinking, product ideation, and innovation methods.

Course Outcomes:

COs	**At the end of successful completion of the course the student will be able to**	**Blooms Taxonomy**
CO1	Understand core concepts of cybersecurity	**Understand**
CO2	Analyze innovation opportunities in the security domain	**Analyze**
CO3	Apply design thinking for cybersecurity problems	**Apply**
CO4	Develop an MVP or concept for a cybersecurity product	**Analyze**

Course Contents

Unit-I	**Fundamentals of Cyber Security**	**08 Hours**

Information security principles (CIA Triad), Types of threats and attacks (malware, phishing, social engineering), Network and application vulnerabilities, Security architecture and design.

Unit-II	**Cybersecurity Innovation Landscape**	**06 Hours**

Major challenges and opportunities in cybersecurity, Emerging trends (Zero Trust, IoT Security, CloudSec, AI/ML in Security), Innovation gap in cyber defense, Case study: How startups disrupt traditional security solutions.

Unit-III	**Introduction to Design Thinking**	**06 Hours**

Design Thinking principles (Empathize, Define, Ideate, Prototype, Test), Applying design thinking to cybersecurity problem-solving, Group activity: Ideation session for campus-related cyber threats.

Unit-IV	**Product Innovation in Cybersecurity**	**07 Hours**

Understanding user pain points in digital security, Ideating security-focused tools and apps, Prototyping frameworks and low-code tools (e.g., Figma, MIT App Inventor), Introduction to MVP (Minimum Viable Product).

Unit-V	**Entrepreneurship Awareness**	**07 Hours**

Concept of entrepreneurship and types, Startups in the cybersecurity domain, Innovation to market: journey of a cyber product, Innovation challenges and government support (MeitY, Startup India).		
Unit-VI	**Student Innovation Showcase**	**07 Hours**
Pitch a security innovation idea, Peer review and faculty feedback, Mentorship activity (industry or incubator connect if available).		

Course delivery methods	Assessment methods
1. Black Board Teaching 2. Power Point Presentation	1. Internal Assessment 2. Assignment 3. Quiz

Text Books

1. "Cybersecurity Essentials" – Charles J. Brooks et al.
2. "Design Thinking for Strategic Innovation" – Idris Mootee

Reference Books

1. "Cybersecurity for Beginners" – Raef Meeuwisse
2. NASSCOM / DSCI Startup Reports

CO-PO Mapping:

PO / CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	--	1	--	--	--	--	--	1	--	--	1
CO2	2	2	--	2	2	--	--	--	--	--	--	1
CO3	2	3	2	1	2	--	--	--	--	--	--	1
CO4	2	3	2	--	1	--	--	--	2	--	--	2

1-Low, 2-Medium, 3-High

----------END----------

Second Year B. Tech(CS) (Semester – III)

25UG-VEC2-CS410: Cyber Ethics & Social Responsibility

Teaching Scheme	Credits :01	Examination Scheme
Lectures: 02 Hrs / Week		**ISA(TW):** 25 Marks

Course Description:

Focuses on entrepreneurial principles, startup lifecycle, funding, and product-market fit in the context of cybersecurity.

Prerequisites:	Professional Ethics and Human Values

Course Objectives:

1. To develop an understanding of ethical principles specific to cyberspace.
2. To examine the social responsibilities of cybersecurity professionals.
3. To analyze legal and ethical challenges in the digital environment.
4. To promote a responsible and accountable approach to digital citizenship.

Course Outcomes:

COs	At the end of successful completion of the course the student will beable to	Blooms Taxonomy
CO1	Understand core concepts of cyber ethics and responsible behavior online.	Understand
CO2	Evaluate ethical dilemmas in cybersecurity practices and policy.	Apply
CO3	Analyze the impact of cybersecurity measures on society and human rights.	Analyze
CO4	Practice responsible digital citizenship and advocate ethical online conduct.	Analyze

Course Contents

Unit-I	Introduction to Cyber Ethics	04 Hours

Definition and significance of cyber ethics, Differences between personal and professional cyber conduct, Introduction to ethical hacking and responsible disclosure.

Unit-II	Ethical Challenges in Cyberspace	08 Hours

Anonymity and accountability, Piracy, plagiarism, and intellectual property violations, Deepfakes, misinformation, and cyberbullying.

Unit-III	Digital Citizenship and Online Behavior	09 Hours

Netiquette and social media ethics, Digital footprints and privacy awareness, Ethics in online collaboration and communication.

Unit-IV	Social Impact of Cybersecurity Policies	07 Hours

Surveillance vs. civil liberties, Inclusion, accessibility, and cybersecurity equity, Case Study: China's Social Credit System and GDPR.

Unit-V	Ethical Risk Assessment in Cybersecurity	06 Hours

Ethical considerations in data collection and surveillance, Ethics in Artificial Intelligence and automation, Developing ethical cybersecurity frameworks.		
Unit-VI	**Promoting Ethical Culture in Organizations**	**06 Hours**
Creating ethical policies for cybersecurity teams, Cybersecurity whistleblowing and reporting, Leadership in promoting cyber ethics.		

Course delivery methods	Assessment methods
1. Black Board Teaching 2. Power Point Presentation	1. Internal Assessment 2. Experiments 3. Quiz

Text Book:

1. Tavani, Herman – Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing, Wiley.
2. Moor, James H. – What is Computer Ethics? (in Readings in Cyberethics)

Reference Books:

1. Spinello, Richard A. – CyberEthics: Morality and Law in Cyberspace, Jones & Bartlett.
2. Deborah Johnson – Computer Ethics, Pearson Education.

CO-PO Mapping:

PO / CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	--	--	--	3	3	8	--	--	--	--
CO2	2	2	--	--	--	3	2	2	--	--	--	--
CO3	--	--	--	--	--	3	3	2	--	--	2	--
CO4	--	--	--	--	--	3	3	3	2	--	2	--

1-Low, 2-Medium, 3-High

Member Secretory Board of Studies Department of Cyber Security Engineering	Chairman Board of Studies Department of Cyber Security Engineering	Dean Academic TKIET (Autonomous) Warananagar	Dean SETM TKIET (Autonomous) Warananagar	Principal TKIET (Autonomous) Warananagar

----------END----------