Solapur University with UDDYAM – PAHSUI Introduces University Grants Commission (UGC) Mandated 4 Credits ENGENEERING PEC-01 3 CREDITS THEORY + 1 CREDIT PRACTICAL		
Title of the Paper		Syllabus for Cybersecurity foundations program (Undergraduate Level)
Mandatory Credits		3+1
From Academic Year		2025-26
Sr No	**Heading**	Particulars
1	**Course Title**	Cybersecurity
2.	**Course Code**	(To be assigned by Solapur University)
3.	**Description of The Program**	The Undergraduate Program in Cyber Security is designed to provide students with a strong foundational understanding of the rapidly evolving digital threat landscape. Through a blend of theoretical modules and practical applications, students explore core topics such as cyberspace architecture, cyber crimes and legal frameworks, digital payment security, social media privacy, and the protection of personal digital devices. Emphasis is placed on understanding modern threats, including phishing, malware, social engineering, and data breaches, as well as developing skills in reporting incidents and configuring security tools. With integrated hands-on labs and real-world case studies, the program equips learners with the knowledge and tools to responsibly navigate digital environments, making it ideal for those pursuing careers in IT, security operations, digital forensics, or cyber law.
4.	Vertical:	✓ Vocational Skill Enhancement / ✓ Value Education Course / ✓ Open Elective
5.	Type	Theory and Practical
6.	Credit	2 credits
7.	Hours allotted	30 hours
8.	Marks allotted	50 marks
9.	**Course Objectives of the Program** • Develop foundational knowledge of cyberspace, web architecture, and digital communication systems while understanding the emerging challenges in cyber security. • Identify and analyze various forms of cyber crimes including social engineering, financial fraud, and cyber threats targeting individuals and organizations, along with relevant legal frameworks such as the IT Act 2000. • Understand and evaluate the role of cyber law, privacy regulations, and policy mechanisms in combating cybercrime and ensuring digital safety. • Examine the security implications of social media usage, including data privacy, inappropriate content, and legal consequences, while adopting best	

	practices for secure digital communication. • Explore the concepts of e-commerce and digital payment systems, including different modes of transactions, threats, and RBI guidelines for secure financial operations. • Learn the principles of digital device security and gain hands-on skills in configuring antivirus, firewalls, password policies, and mobile device security. • Acquire the ability to use practical tools and techniques to report, prevent, and mitigate cyber incidents, and foster a responsible and ethical approach to personal and professional digital interactions.
10.	**Program Outcomes** After completing the Cyber Security Undergraduate Program, students will: • Develop a foundational understanding of cyberspace, digital infrastructure, and the critical role of cybersecurity in the modern digital world. • Recognize and categorize various types of cybercrimes, including online frauds, phishing, ransomware, and social engineering attacks. • Gain knowledge of national cyber laws and regulations, especially the IT Act 2000, and understand how to report and respond to cyber incidents. • Understand the security and privacy challenges associated with social media platforms and apply best practices for responsible digital behaviour. • Acquire familiarity with e-commerce systems and digital payment modes, along with the ability to recognize and prevent associated frauds. • Develop hands-on proficiency in securing digital devices through password policies, antivirus tools, firewalls, and mobile security settings. • Implement basic cybersecurity tools and technologies to detect threats and apply remedial measures to protect personal and institutional data. • Demonstrate the ability to configure, manage, and monitor endpoint device security, and apply guidelines to mitigate risks. • Strengthen their awareness of ethical issues in digital interactions and data usage, fostering responsible digital citizenship. • Gain experience in practical applications through case studies and lab exercises that simulate real-world cyber scenarios. • Prepare for entry-level roles in cybersecurity support, digital risk awareness, IT help desk functions, and cyber law consultancy. • Build a strong foundation to pursue higher education or certifications in cybersecurity, digital forensics, ethical hacking, or information security management.
11.	**Modules: 3 CREDITS** **Our course content is designed based on the UGC syllabus, ensuring academic relevance and quality.**
Module 1: Introduction to Cyber security	
	Module Content - Defining Cyberspace and Overview of Computer and Web-technology, Architecture of cyberspace, Communication and web, Internet, World wide web, Advent of internet, Internet infrastructure for data transfer and governance, Internet society, Regulation of cyberspace, Concept of cyber security,

	Issues and challenges of cyber security. Basic cybersecurity principles: Confidentiality, Integrity and Availability (CIA Triad) Common types of cyber threats faced by individuals and organizations
	Learning Outcomes - After completion of this module, students would be able to understand the concept of Cyber security and issues and challenges associated with it. Explain basic security principles used to protect digital information
Module 2: Cybercrime and Cyber law	
	Module Content - Classification of cyber crimes, Common cyber crimes- cyber crime targeting computers and mobiles, cyber crime against women and children, financial frauds, social engineering attacks, malware and ransomware attacks, zero day and zero click attacks, Cybercriminals modus-operandi ,Reporting of cyber crimes, Remedial and mitigation measures, Legal perspective of cyber crime, IT Act 2000 and its amendments, Cyber crime and offences, Organisations dealing with Cyber crime and Cyber security in India, Case studies. Online frauds such as phishing, vishing and smishing National Cyber Crime Reporting Portal
	Learning Outcomes - Students, at the end of this module, should be able to understand the cyber crimes, their nature, legal remedies and as to how report the crimes through available platforms and procedures.
	Practical – 1. Reporting phishing emails. 2. Demonstration of email phishing attack and preventive measures.
Module 3: Social Media Overview and Security	
	Module Content - Introduction to Social networks. Types of Social media, Social media platforms, Social media monitoring, Hashtag, Viral 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. Digital footprint and online reputation Risks of oversharing personal information

	Learning Outcomes - On completion of this module, students should be able to appreciate various privacy and security concerns on online Social media and understand the reporting procedure of inappropriate content, underlying legal aspects and best practices for the use of Social media platforms.
	Practical – 1. Reporting and redressal mechanism for violations and misuse of Social media platforms.
Module 4: E - Commerce and Digital Payments	
	Module Content - Definition of E- Commerce, Main components of E-Commerce, Elements of E-Commerce security, E-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 unauthorised banking transactions. Relevant provisions of Payment Settlement Act,2007 Two-factor authentication used in digital payments
	Learning Outcomes - After the completion of this module, students would be able to understand the basic concepts related to E-Commerce and digital payments. They will become familiar with various digital payment modes and related cyber security aspects, RBI guidelines and preventive measures against digital payment frauds.
	Practical – 1. Configuring security settings in Mobile Wallets and UPIs.
Module 5: Digital Devices Security, Tools and Technologies for Cyber Security	
	Module Content - 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. Importance of strong passwords and multi-factor authentication Safe use of public Wi-Fi networks
	Learning Outcomes - Students, after completion of this module will be able to understand the basic security aspects related to Computer and Mobiles. They will be able to use basic tools and technologies to protect their devices.
	Practical – 1. Setting, configuring and managing three password policy in the computer (BIOS, Administrator and Standard User).

	2. Security patch management and updates in Computer and Mobiles. 3. Managing Application permissions in Mobile phone. 4. Installation and configuration of computer Anti-virus. 5. Installation and configuration of Computer Host Firewall.
13.	**Modules: 1 CREDIT PRACTICAL** **Our course content is designed based on the UGC syllabus, ensuring academic relevance and quality.**
	Practical Module 1: Phishing and Email Security Experiments: 1. Identify phishing emails using real sample emails. 2. Analyse suspicious email headers and sender addresses. 3. Report phishing emails through email clients and cybercrime portals. 4. Demonstrate how phishing attacks trick users (educational simulation). Learning Outcome Students will learn how phishing attacks work and how to identify fraudulent emails. Practical Module 2: Cybercrime Reporting Mechanisms Experiments: 1. Explore the **National Cyber Crime Reporting Portal**. 2. Submit a mock cybercrime complaint. 3. Document required information for reporting cyber fraud. 4. Understand procedures followed by cyber police stations. Learning Outcome Students will learn how cyber incidents are reported and handled in India. Practical Module 3: Social Media Privacy and Safety Experiments: 1. Configure privacy settings on major social media platforms. 2. Identify fake accounts and suspicious profiles. 3. Report inappropriate content and abusive behaviour. 4. Analyse digital footprints created by social media activity. 5. Review case studies of social media misuse. Learning Outcome Students will learn to secure social media accounts and understand privacy risks.

Practical Module 4: Digital Payment Security

Experiments:

1. Configure security settings in **UPI applications**.
2. Configure security features in **mobile wallets**.
3. Enable two-factor authentication in digital payment apps.
4. Identify signs of digital payment fraud.
5. Study common online banking fraud scenarios.

Learning Outcome
Students will understand safe practices when using digital payment systems.

Practical Module 5: Password and Authentication Security

Experiments:

1. Create strong password policies.
2. Configure BIOS password in a system.
3. Configure administrator and standard user accounts.
4. Demonstrate password management practices.

Learning Outcome
Students will understand secure authentication practices and password management.

Practical Module 6: Computer System Security

Experiments:

1. Install and configure antivirus software.
2. Perform system scan and malware detection.
3. Configure host firewall settings.
4. Update operating system security patches.

Learning Outcome
Students will learn how to secure computers using built-in security tools.

Practical Module 7: Mobile Device Security

Experiments:

1. Manage application permissions on mobile devices.
2. Identify potentially harmful applications.
3. Configure mobile security settings.

	4. Enable device lock and biometric security. Learning Outcome Students will learn to secure their smartphones and prevent unauthorized access.
14.	**REFERENCES** 1. Cyber Crime Impact in the New Millennium, by R. C Mishra, Auther Press. Edition 2010. 2. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011) 3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001) 4. Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd. 5. Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers. 6. Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd. 7. Fundamentals of Network Security by E. Maiwald, McGraw Hill.
15.	**Semester-End Examination -** MCQ-based online exam conducted through the LMS. The question paper is for 100 marks. Minimum 40 marks required to pass.
16.	**Format of question paper: Multiple Choice Questions (MCQs)**
17.	**Live Sessions and Course material -** There is no live online sessions. The entire course is self-study-oriented in accordance with the syllabus prescribed by the UGC. It includes E- book, recorded videos, lab manual, and assignments. The course is made available completely online through the LMS, allowing students to explore the content in a self-paced manner.