AC – 28/03/2025
Item No. – 6.2 (N) (2a) Sem. IV

As Per NEP 2020

University of Mumbai

Syllabus for Basket of OE Vertical 3	
Faculty of Science and Technology	
Board of Studies in Information Technology	
Second Year Programme	
Semester	**IV**
Title of Paper	**Credits**
Cyber Security	**2**
From the Academic Year	**2025-26**

Title of Paper Cyber Security

Sr.No.	Heading	Particulars
1	Description the course : Including but Not limited to:	A Cybersecurity course focuses on teaching students how to protect and secure systems, networks, and data from unauthorized access, attacks, and damage. It covers a range of topics that equip students with the skills and knowledge to identify security vulnerabilities, mitigate risks, and respond to cybersecurity incidents. This course is suitable for anyone looking to build a career in IT security or for professionals who want to deepen their understanding of the security challenges in the digital age
2	Vertical :	Open Elective for Others
3	Type :	Theory
4	Credits :	2 credits (1 credit = 15 Hours for Theory in a semester, Total 30 hours)
5	Hours Allotted :	30
6	Marks Allotted:	50
7	Course Objectives(CO): CO 1: Understand cybersecurity fundamentals, ethical practices, and privacy considerations. CO 2: Identify threats, phishing tactics, and malware while applying mitigation strategies. CO 3: Secure systems and networks using authentication, firewalls, and intrusion prevention. CO 4: Apply cryptographic methods like encryption, hashing, and key management. CO 5: Develop and implement risk management strategies for enhanced cybersecurity resilience.	
8	Course Outcomes (OC): OC 1. Gain practical skills to detect and prevent cybersecurity threats. OC 2: Understand the mindset and methodologies of attackers. OC 3: Be capable of applying cybersecurity techniques to safeguard networks, systems, and data. OC 4:Develop a proactive approach to mitigate risks and enhance organizational resilience.	
9	Modules:- Module 1:	
	Unit 1: Fundamentals of Cybersecurity and Threat Landscape 1. Introduction to Cybersecurity	15 Hrs

	What Is Cybersecurity? Cybersecurity and Privacy, What Cybersecurity Isn't, Black Hats vs. White Hats, Types of Black Hats, Types of White Hats, Exercise: Learning More About Cybersecurity and Threats 2. Attack Targets on the Internet How the Internet Works, TCP/IP: The Backbone of the Internet, Public vs. Private Networks, How the Internet Looks to a Black Hat, The Black Hat Attack Methodology: Reconnaissance Weaponization Delivery Exploitation and Installation Command and Control Attack on Objectives, How Black Hats Find You, Examples: The Merger Social Media Hunting, How to Hide from Black Hats, The Internet Is Open, Public, and Forever, Exercise: Analyzing Your Network, Network Command Line Tools, Using Shodan 3. Phishing Tactics What Is Phishing? An Obvious Phish , Not All Phishing Is Obvious , Using Details for a More Convincing Phish , Vishing and Other Non-Email Phishing ,How to Protect Yourself Against Phishing How Black Hats Trick You with URLs : Typosquatting Complex URLs and Redirects Modifying DNS Records ,Hoaxes ,Why Black Hats Love Phishing ,Preventive Measures: Think Twice to Avoid Phishing Take an Alternate Route Listen to Your Spidey Sense ,Exercise: Analyzing a Phishing Email, Phishing Email Indicators, Header Analysis, URL Analysis 4. Malware Infections What Is Malware? Types of Malware: Viruses, Worms, Trojans, Ransomware, Spyware, and Adware Rootkits and Bootkits Polymorphic, Malware How Black Hats Deploy Malware How to Defend Against Malware Exercise: Analyzing Malware and Managing Antivirus Settings	
	Module 2:	
	Unit 2: Advanced Cybersecurity Techniques and Countermeasures 1. Password Thefts and Account Access Tricks Authentication and Types of Authentication, Multi-Factor Authentication Authorization Models: Mandatory Access Control, Rule-Based, Role-Based, Attribute-Based, and Discretionary Access Control, Accounting: Logging and Auditing Indicators of Attack, Exercise: Setting Up Accounts in Windows and macOS 2. Network Tapping and Attacks Basics of Network Design, How Black Hats See Your Traffic, Network Attacks: Man-in-the-Middle Attacks Denial of Service (DoS) and Distributed Denial of Service (DDoS), Defense Against Network Attacks:	15 Hrs

	Firewalls, Intrusion Detection Systems (IDS) Intrusion Prevention Systems (IPS) Exercise: Setting Up Your Firewall (Windows/macOS) 3. Attacks in the Cloud How Cloud Computing Works: SaaS, PaaS, IaaS, Security as a Service Attacking and Defending the Cloud, Web Application Attacks and Countermeasures, Exercise: Performing SQL Injection on the Damn Vulnerable Web Application 4. Wireless Network Pirating How Wireless Networks Work, Wireless Standards and Security Wireless Authentication and Encryption, Wireless Attacks: Rogue Access Points Disassociation Attacks Jamming, Setting Up a Secure Wireless Network, Exercise: Secure Your WAP 5. Encryption Cracking Introduction to Cryptography: Early and Modern Cryptography Symmetric vs. Asymmetric Cryptography Validating Public Keys Hashing, Cryptanalysis: Asymmetric Algorithm Attacks Breaking Hashes Defensive Measures: Salting Hashes Protecting Encryption Keys Exercise: Encrypting and Hashing Files 6. Defeating Black Hats Risks, Threats, and Controls, Risk Management Programs, Putting It All Together, Exercise: Conducting a Risk Analysis	
10	Books and References: 1. How Cybersecurity Really Works A Hands-On Guide for Total Beginners By Sam Grubb 1st Edition Publisher: No Starch Press 2021 2. Cybersecurity: The Beginner's Guide - A comprehensive guide to getting started in cybersecurity by Dr. Erdal Ozkaya Publisher Packt Publishing 2019 3. Cybersecurity Essentials by Charles J. Brooks, Christopher Grow, Philip A. Craig, Jr., Donald Short Publisher: John Wiley & Sons, 2018 4. Cybersecurity All-in-one for Dummies by Joseph Steinberg , Kevin Beaver , Ira Winkler , Ted Coombs 1sr Edition Published by: John Wiley & Sons, Inc 2023	
12	Internal Continuous Assessment: 40%	Semester End Examination: 60%
13	Continuous Evaluation through: Class test of 1 of 15 marks Class test of 2 of 15 marks Average of the two: 15 marks Quizzes/ Presentations/ Assignments: 5 marks Total: 20 marks	Format of Question Paper: External Examination (30 Marks)– 1 hr duration

14	Format of Question Paper: (Semester End Examination: 30 Marks. Duration:1 hour) Q1: Attempt any two (out of four) from Module 1 (15 marks) Q2: Attempt any two (out of four) from Module 2 (15 marks) Or Q1: Attempt any three (out of five) from Module 1 (15 marks) Q2: Attempt any three (out of five) from Module 2 (15 marks)

Sd/-	**Sd/-**	**Sd/-**
Sign of the BOS Chairman	**Sign of the Offg. Associate Dean**	**Sign of the Offg. Dean**
Dr. Srivaramangai R	**Dr. Madhav R. Rajwade**	**Prof. Shivram S. Garje**
BOS in Information Technology	**Faculty of Science & Technology**	**Faculty of Science & Technology**