Hindi Vidya Prachar Samiti's

Ramniranjan Jhunjhunwala College

of Arts, Science & Commerce

(Empowered Autonomous College)

Affiliated to

UNIVERSITY OF MUMBAI

Program Code: RJCUCSDF

Syllabus for the

B.Sc Cyber Security & Digital Forensics (under NEP)

Course Codes: RJSECCSDF111 & RJSECCSDF121

New Program to be started from the academic year 2026-2027

Preamble

The National Education Policy 2020 aims at imparting skill-based learning and caters to the multiple entry and exit facility for the students thus empowering them to acquire knowledge at their pace In the three-year UG program, the student has two exit options. Students also have the option for choosing the Honors program of four years study in a given discipline and later converting it to five year integrated PG degree program. As undergraduate student, he/she learns the core subject (Major), subject complementing the core subject (Minor), a course from other discipline (OEC or GEC) Vocational and Skill Enhancement course from the Major(VSEC). The remaining verticals under NEP 2020 are IKS (Indian Knowledge System), AEC (Ability Enhancement Course), VEC (Value Enhancement Course) and with progressive three years of UG, student also completes at different levels OJT (On Job Training), FP (Field Projects), CEP (Community Engagement Program) , RP (Research Project) which helps him/her in understanding their roots, application of the knowledge for the benefit of self and the society. Vertical CC (Co-curricular activities and activities related to yoga and human well-being) helps in preparing youth with good character and interpersonal relationships.

SEMESTER I

Skill Enhancement (SEC) – Introduction to Cyber Threats

Course Code	Course Title	Course Type	Credits	Hours
• RJSECCSDF111	Introduction to Cyber Threats	Skill Enhancement (Theory)	2	30

Course Objectives

Sr. No.	Course Objective
1	Understand common cyber threats and attack vectors, including their impact on confidentiality, integrity, and availability.
2	Explain malware types, propagation methods, and basic mitigation strategies.
3	Learn social engineering techniques, such as phishing, and recognition methods.
4	Explore insider threats, supply chain risks, and detection indicators.
5	Develop awareness of threat intelligence basics and simple modeling frameworks.

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
I	Overview of Cyber Threats • Threat Landscape: Introduction to cybersecurity fundamentals, CIA triad (Confidentiality, Integrity, Availability), common attack surfaces (e.g., endpoints, networks). • Malware Fundamentals: Types of malware (viruses, worms, trojans, ransomware) – Definitions, examples, and real-world impacts on systems and data. • Network-Based Threats: DDoS attacks, Man-in-the-Middle (MITM), SQL injection – Mechanisms, symptoms, and basic consequences. Practical of Malware Identification: Simulate malware detection using online scanners or virtual sandboxes (e.g., VirusTotal integration or simple demo files in a safe environment using Simulators / Virtual Labs).	15
II	Human-Centric and Advanced Threats • Social Engineering: Techniques including phishing, vishing, pretexting – Psychological manipulation, common signs, and defensive awareness. • Insider and Supply Chain Threats: Types of insider threats (intentional vs. unintentional), supply chain vulnerabilities (e.g., third-party software risks) – Detection indicators and prevention basics.	15

	• Advanced Persistent Threats (APTs): Zero-day exploits, nation-state actors – Lifecycle overview and high-level response strategies. • Threat Modeling: Introduction to STRIDE framework (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) – Simple application to scenarios. Practical of Threat Simulation: Model a basic phishing attack or insider threat scenario using role-playing tools or virtual labs (e.g., phishing email simulator or STRIDE worksheet in Simulators / Virtual Labs).	

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Describe types of malware and network threats, including their mechanisms and impacts.	Remember (L1), Understand (L2)	PSO1, PSO5
CO2	Explain social engineering attack methods and basic recognition strategies.	Understand (L2)	PSO1, PSO3, PSO5
CO3	Identify insider, supply chain, and APT risks in organizational contexts.	Understand (L2), Apply (L3)	PSO1, PSO3, PSO5
CO4	Analyze threat scenarios using introductory modeling frameworks like STRIDE.	Apply (L3), Analyze (L4)	PSO1, PSO2, PSO3, PSO5
CO5	Recognize emerging cyber threats and simulate basic defenses in virtual environments.	Understand (L2), Analyze (L4)	PSO1, PSO3, PSO5

Textbooks & References

Sr. No.	Title	Author / Source
1	Cybersecurity and Cyberwar (2014)	P.W. Singer, Allan Friedman / Eamon Dolan
2	Hacking Exposed (8th Ed., 2023)	Stuart McClure et al. / McGraw-Hill
3	Cyber Threat Intelligence (2018)	Ali Dehghantanha, Kim-Kwang Raymond Choo / Springer
4	The Fifth Domain (2019)	Richard A. Clarke, Robert K. Knake / Penguin Press

5	Worm: The First Digital World War (2013)	Mark Bowden / Atlantic Monthly Press

SEMESTER II

Skill Enhancement – Web Technology Fundamentals

Course Code	Course Title	Course Type	Credits	Hours
RJSECCSDF121	Web Technology Fundamentals	Skill enhancement (Theory)	2	30

Course Objectives

Sr. No.	Course Objective
1	Understand HTML structure and CSS styling for secure web pages.
2	Learn JavaScript basics for interactive client-side scripting.
3	Explore client-server architecture and basic HTTP protocols.
4	Apply forms, events, and dynamic content for user interactions.
5	Develop awareness of web vulnerabilities like XSS and secure coding.

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
I	• Web Basics • HTML5 Fundamentals: Semantic elements (article, section), tables for data display (e.g., threat matrix), forms (text, radio, submit buttons) with validation attributes. • CSS3 Styling: Inline/internal/external stylesheets; selectors (element, class, ID); box model (margin, padding, border); basic layouts (inline-block, float). Practical Tasks: (1) Build HTML page with form for login; add table for user list. (2) Style page with CSS colors/fonts; create responsive divs. (3) Embed image/link for security icons. Tool: VS Code with Live Server.	15
II	• Advanced Web and Security • JavaScript Essentials: Variables (let/const), functions (arrow), DOM methods (querySelector, addEventListener); events (click, submit). • Client-Server Model: HTTP methods (GET/POST), status codes (200, 404); intro to APIs (JSON response). • Web Security: XSS (script injection), CSRF (token prevention); secure coding (escape outputs, HTTPS). Practical Tasks: (1) JS to validate form on submit (e.g., email pattern). (2) Dynamic DOM: Add/remove list items on button click. (3) Simulate secure fetch to mock API; alert on errors. Tool: VS Code with Live Server.	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Describe HTML/CSS/JS elements for web structure.	Remember (L1), Understand (L2)	PSO1, PSO5
CO2	Explain client-server protocols and dynamic scripting.	Understand (L2)	PSO1, PSO3, PSO5
CO3	Apply forms and events for interactive secure pages.	Understand (L2), Apply (L3)	PSO1, PSO3, PSO5
CO4	Analyze web vulnerabilities and mitigation codes.	Apply (L3), Analyze (L4)	PSO1, PSO2, PSO3, PSO5
CO5	Identify best practices for secure web development.	Understand (L2), Analyze (L4)	PSO1, PSO3, PSO5

Textbooks & References

Sr. No.	Title	Author / Source
1	HTML and CSS: Design and Build Websites	Jon Duckett / Wiley
2	Eloquent JavaScript (3rd Ed., 2018)	Marijn Haverbeke / No Starch Press
3	Web Application Security (2nd Ed.)	Andrew Hoffman / O'Reilly
4	Web Technologies: A Computer Science Perspective	Jeffrey C. Jackson / Pearson
5	Web Tech Lab Manual (B.Sc. IT, Mumbai University)	Various / Internal Publication