Savitribai Phule Pune University

B. Sc. (Cyber Security)

(To be implemented from Academic year 2024-2025)

1. Name of Program: Cyber Security

2. Introduction:

In today's interconnected world, the proliferation of digital technologies has brought about unprecedented convenience and efficiency. However, this digital transformation has also led to an increase in cyber threats, making cyber security an essential field. Cyber-attacks can cause significant harm to individuals, businesses, and national security. As a result, there is a growing demand for skilled cyber security professionals who can protect sensitive information and critical infrastructure.

The B.Sc. in Cyber Security program is designed to address this demand by providing students with a comprehensive education in the field. Aligned with the National Education Policy (NEP) 2020, this program emphasizes a holistic, flexible, and multidisciplinary approach to education, preparing students for the complexities of the cyber security landscape.

The Program is of Three Years duration with six semesters. It is a Full-Time Degree Program. The program will be based on the Choice-based credit system comprising 140 credit points.

3. Objectives:

- To Develop Proficiency in Cyber Security: Equip students with the skills to protect Information systems against cyber threats and vulnerabilities.
- To provide hands-on experience with current security technologies and tools.
- To an understanding of the ethical, legal, and societal implications of cyber security practices.
- To encourage innovative problem-solving and critical analysis of security issues.
- To develop an understanding of the global context and cultural dimensions of cyber security

4. **Eligibility:**
   - Higher secondary school certificate (10+2) or its equivalent examination with English

     OR
   - Three-year diploma course from the board of technical education conducted by Government of Maharashtra or its equivalent

     OR
   - Higher secondary school certificate (10+2) Examination with English and avocational subject of +2 level (MCVC)

PO No.	PO Outcomes
PO1	Become proficient in Linux administration, as it is essential in today's IT environment.
PO2	Address and take action to meet the cyber security needs of the modern IT world.
PO3	Cultivate creative abilities, critical thinking, analytical skills, and research capabilities to tackle real-world problems using cyber security expertise.
PO4	Understand the Concepts of cyber security, Networking and vulnerability testing and statistical methods.
PO5	Applying the Concepts of Digital Communication and IOT.
PO6	Identify and evaluate software vulnerabilities and security solutions to mitigate the risk of exploitation.
PO7	Acquire essential programming languages such as C and Python
PO8	Integrate ethics and cyber laws to understand the rules and regulations of the current IT environment.
PO9	To developing regulations and tactics for cyber security
PO10	Cloud security protects applications, data, and cloud-based infrastructure.
PO11	Comprehend security concepts such as cyber threat intelligence, block chain in cyber security, communication systems security, malware analysis, vulnerability assessment and penetration testing (VAPT), intrusion detection and prevention systems (IDS & IPS), and cybercrime reporting.