**Course Curriculum**

1. Introduction to Cyber security, Definition of cyber security, Importance and relevance of cyber security,

Evolution of cyber security threats.

1. Security Principles and Concepts: Confidentiality, integrity, availability (CIA) triad, Defense-in-depth,

Least privilege principles.

1. Threats and Attack Vectors; Malware (viruses, worms, Trojans, ransom ware), Social engineering,

Phishing and spear-phishing attacks, Denial-of-service (DoS) and distributed denial-of-service

(DDoS) attacks.

1. Cryptography Basics: Encryption algorithms (symmetric vs. asymmetric), Public

Key infrastructure (PKI), Digital signatures and certificates.

1. Authentication and Access Control; Passwords and multi-factor authentication, Role-based access

Control (RBAC), Biometric authentication.

1. Network Security, Firewalls and intrusion detection/prevention systems (IDS/IPS), Virtual private

Networks (VPNs), Secure Socket Layer/Transport Layer Security (SSL/TLS).

1. Risk Management, Risk assessment and analysis, Risk mitigation strategies, Incident response

Planning, Secure System Configuration and Maintenance;

1. Patch management, secure coding practices, Data backup and recovery,
2. Ethical, Legal, and Societal Issues, Privacy considerations, Compliance regulations (e.g., GDPR, HIPAA),

Cybersecurity ethics.

1. Case Studies and Practical Exercises, Analysis of real-world security breaches, Hands-on labs to

Reinforce concepts, Simulation exercises for incident response.

1. Security Principles and Practices in Linux; Understanding the Linux security model, File permissions and

Access control in Linux, Threats and Vulnerabilities in Linux Systems, Common Linux vulnerabilities,

Linux-specific malware and exploits.