PGCP in Cyber Security

Duration – 160 Hours

Program Description

This program provides an end-to-end understanding of cybersecurity principles, practices, and tools. It equips learners with the skills to protect digital assets, secure networks and applications, implement cryptography, manage identity and access, conduct penetration testing, and respond to cyber incidents. The curriculum integrates foundational concepts, modern threat landscapes, secure software development, cloud security, and AI/ML-driven threat detection, preparing participants for real-world security challenges.

Learning Goals

- Understand the fundamentals of cybersecurity, including vulnerabilities, threats, and risk management
- Gain proficiency in network, web, and application security
- Learn programming basics relevant to security
- Apply cryptography, encryption, and public key infrastructure principles
- Implement secure SDLC practices and software security testing
- Conduct penetration testing, malware analysis, and API/security auditing
- Manage identity, authentication, and access control effectively
- Understand regulatory compliance, business continuity, disaster recovery, and SOC operations
- Secure cloud environments and emerging technologies
- Develop incident response, monitoring, and threat intelligence capabilities

PGCP in Cyber Security

Duration – 80 Hours

Course Topics

- Introduction to Cybersecurity
- Networking and Web Fundamentals
- Programming for Security
- Secure Network Architecture
- Cryptography
- Laws, Regulations & Compliance
- Personnel Security & Risk Management
- Asset Security & Security Models
- Secure Communications & Network Protection
- Identity & Access Management
- Secure SDLC
- Malicious Code & Application Attacks
- MERN/PERN Security
- Business Continuity & Disaster Recovery
- Advanced Threats & Kill Chain
- Advanced Penetration Testing & Red Teaming
- Security Operations & Incident Response
- Industrial, OT & Supply Chain Security
- Cloud Security
- AI/ML in Cybersecurity