SYLLABI

For

Value Added Course

Certificate Course in Cyber Security

Offered by

Department of Information Communication and Technology

TECNIA INSTITUTE OF ADVANCED STUDIES

NAAC ACCREDITED GRADE 'A' INSTITUTE

3 PSP, Institutional Area, Sector – 14, Rohini, Delhi - 110085

Course Module

For

Value Added Course

Course Structure

S.No.	Contents Deliverance	Learning Outcomes
1	Introduction to cyber security (2 Hrs)	Understand the fundamentals of cyber security, including key terminologies, concepts, and principles.
2	Cyber security assurance framework (3 Hrs)	Identify common types of cyber threats and attacks, including malware, phishing, social engineering, and denial of service (DoS).
3	Desktop security and malware (2 Hrs)	Analyze and assess vulnerabilities in computer systems, networks, and applications to identify potential security risks.
4	E-commerce and web-application security (2 Hrs)	Implement security measures and controls to protect computer systems, networks, and data from unauthorized access and malicious activities.
5	Social engineering (2Hrs)	Configure and manage network security devices, such as firewalls, intrusion detection systems (IDS), and virtual private networks (VPNs).
6	Cyber security risk management (2 Hrs)	Understand and implement cryptographic techniques, including encryption, hashing, and digital signatures, to secure data transmission and storage.
7	Awareness of Legal and Ethical Considerations (2 Hrs)	Conduct security assessments and penetration testing to identify weaknesses and vulnerabilities in computer systems and networks.
8	Computer forensics fundamentals and collection of digital evidence (4 Hrs)	Develop incident response plans and procedures to effectively respond to and mitigate security incidents.
9	Cyber security initiatives in India (3 Hrs)	Understand legal and ethical considerations in cyber security, including privacy laws, intellectual property rights, and ethical hacking guidelines.
10	Cyber security strategies and	Stay updated with the latest cyber security

	policies (2 Hrs)	threats, trends, and best practices to proactively address emerging risks.
11	Awareness of Emerging Trends and Technologies (3 Hrs)	Understand the principles of secure software development and apply secure coding practices to develop resilient and secure applications.
12	Proficiency in Secure Cloud Computing (3 Hrs)	Analyze security logs and monitor network traffic to detect and respond to security incidents.

Reference:

1. The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders, and Deceivers" by Kevin D. Mitnick and William L. Simon, December 2005
2. Network Security: Private Communication in a Public World" by Charlie Kaufman, Radia Perlman, and Mike Speciner, April 2002
3. CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide" by Mike Chapple, James Michael Stewart, and Darril Gibson, June 2021
4. The Practice of Network Security Monitoring: Understanding Incident Detection and Response" by Richard Bejtlich, July 2013
5. Cybersecurity: The Essential Body of Knowledge" edited by Dan Shoemaker and Wm. Arthur Conklin, May 2011

Evaluation Pattern: On the basis of practical exam followed by viva.