TECNIA INSTITUTE OF ADVANCED STUDIES
NAAC ACCREDITED GRADE "A" INSTITUTE
Approved by AICTE, Ministry of Education. Govt. of India, Affiliated to GGSIP University
Recognized Under Sec. 2(f) of UGC Act 1956
INSTITUTIONAL AREA MADHUBAN CHOWK,ROHINI,DELHI 110085
Tel:91-11-27555121-24, E-Mail : directortias@tecnia.in, Website: www.tiaspg.tecnia.in

EGAC
Accredited
ISO
21001:2018   51001:2018

TIAS/ACl/2021-22/37   Date:31/12/2021

Course Completion Certificate

This is to certify that the course module for the Certificate Course in Cyber Security scheduled from 13/12/21 to 30/12/21 , comprising of 30 Hours, running in 2 batches deliverance has been completed by the resource person Mr. Harsh, with the module contents as under:-

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 policies (2 Hrs)	Stay updated with the latest cyber security 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.

All the above contents are delivered to the best of my knowledge and belief and nothing is withheld.

Signature
Name of Faculty: Mr. Harsh

Submitted to HoD- Department of Information Communication and Technology, TIAS