Skill India
कौशल भारत-कुशल भारत

Directorate General of Training

सत्यमेव जयते

GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT & ENTREPRENEURSHIP
DIRECTORATE GENERAL OF TRAINING

COMPETENCY BASED CURRICULUM

CERTIFICATE COURSE ON

BASICS OF CYBER SECURITY

NSQF LEVEL- 3.5

SECTOR – IT & ITES

BASICS OF CYBER SECURITY

Duration: 240 Hours

NSQF LEVEL- 3.5

(Version: 1.0)

Designed in 2024

Developed By

Ministry of Skill Development and Entrepreneurship

Directorate General of Training

&

CENTRAL STAFF TRAINING AND RESEARCH INSTITUTE

EN-81, Sector-V, Salt Lake City,

Kolkata – 700 091

CONTENTS

1. COURSE INFORMATION

1.1 GENERAL

This course has been developed for CTS/CITS trainees to take up as optional courses during course of study for technical and behavioural upgradation of trainees to meet industry related job roles. During the 240 hours duration of Cyber Security course, a candidate is trained on professional skills & knowledge related to job role. The Broad components covered during the course are given below:

During the course, trainee will learn about the cyber security including computer network, vulnerability assessments, password managements, firewall and intrusion, cloud security, ethical hacking, social engineering, network traffic analysis, penetration testing, network monitoring tools etc. which are required to handle cyber security aspects requires in current professional world.

1.2 COURSE STRUCTURE

Table below depicts the distribution of training hours across various course elements during a period of 6 weeks: -

S No.	Course Element	Notional Training Hours
1.	Professional Skill (Trade Practical)	180
2.	Professional Knowledge (Trade Theory)	60
	Total	**240**

1.3 ASSESSMENT & CERTIFICATION

The trainee will be tested for his skill, knowledge and attitude during the period of course through assessment at the end of the course through skill testing at Training Center & CBT through examination conducted by DGT.

The minimum pass percentage for skill test is 60% and for theory will be 33% as in main CTS examination.

2. JOB ROLE

Brief description of Job roles:

This course is designed for Trainees who want to get the knowledge and skills of a cyber security professional in today's world. The course comprises of Internet, computer network, vulnerability assessments, password managements, firewall and intrusion, cloud security, ethical hacking, social engineering, network traffic analysis, penetration testing, digital forensics, network monitoring tools etc. After completion of the course, trainees will be ready to meet day to day challenges found in Cyber Security domain related to IT.

Security Analyst: Security Analyst is responsible for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction. They also need to ensure the confidentiality, integrity and availability of data to the 'right' users within/outside of the organization.

Computer Security Specialist: regulates access to computer data files, monitors data file use, and updates computer security files: Enters commands into computer to allow access to computer system for employee who forgot password. Reads computer security files to determine whether denial of data access reported by employee is justified. Modifies security files to correct error, or explains that employee authorization does not permit access. Answers employee questions about computer security. Modifies security files to add new employees, delete former employees, and change employee name, following notice received from computer user departments and personnel office. Send printouts listing employee data authorization to computer user departments to verify or correct in formation in security files. Reviews data use records and compares user names listed in records with employee authorization to ensure that all employees who accessed data files were entitled to do so. Deletes data access of unauthorized users, and for users who have not used data for specified time.

Reference NCO-2015:

i) 2522.0201 - Security Analyst
ii) 3513.0200 - Computer Security Specialist

Mapped NOS: SSC/N9558

3. GENERAL INFORMATION

Name of the Trade	**BASICS OF CYBER SECURITY**
Reference NCO – 2015	2522.0201, 3513.0200
NOS Covered	SSC/N9558
NSQF Level	3.5
Duration of Craftsmen Training	240 Hours
Entry Qualification	10th Class passed and pursuing/ passed out COPA, DBSA, CHNM, ICTSM, Software Testing Assistant, IT, DTPO, MASE under CTS OR CSA, CHNM, DTPO, IT, MASE under CITS Candidates
Unit Strength (No. of Student), Space & Power Norms	Same as COPA / IT / CHNM / ICTSM / DBSA / DTPO / MASE under CTS OR CSA / CHNM / IT / DTPO under CITS.
Instructors Qualification	B.Voc/Degree in Computer Science/ Information Technology from AITCE/UGC Recognized University with one year experience in the relevant field. OR Post Graduate in Computer Science /Computer Application / IT from UGC Recognized University or NIELIT B Level with one-year experience in the relevant field. OR Bachelor in Computer Science / Computer Application / ITOR PGDCA from UGC recognized University or NIELIT A Level with two-year experience in the relevant field. OR 03 years Diploma in Computer Science / IT from recognized Board/ Institute or relevant Advanced Diploma (Vocational) (ADIT) from DGT with two-year experience in the relevant field. OR NTC/NAC in Cyber Security trade with three-year experience in the relevant field.
List of Tools and Equipment	As per Annexure – I

4. LEARNING OUTCOME

Learning outcomes are a reflection of total competencies of a trainee and assessment will be carried out as per the assessment criteria.

4.1 LEARNING OUTCOMES

1. Familiarize with fundamentals of cyber security.
2. Familiarization to recent cybercrime incidents and related Laws to protect.
3. Perform vulnerability assessments on sample systems.
4. Familiarize to different security control mechanisms.
5. Perform cyber-attack simulations.
6. Implement encryption techniques on sample data and analyze the results.
7. Set up and configure firewalls and intrusion detection systems.
8. Familiarize with Social Engineering attacks.
9. Familiarize with ethical hacking.
10. Perform network traffic analysis and identify potential threats.
11. Simulate incident response scenarios and develop incident response plans.

5. SYLLABUS

SYLLABUS – BASICS OF CYBER SECURITY			
Duration: 240 Hours			
Duration Weeks	**Reference Learning outcome**	**Professional Skills (Trade Practical)**	**Professional Knowledge (Trade Theory)**
Professional skills 25 Hrs. Professional Knowledge 05 Hrs.	LO-1: Familiarize with fundamentals of cyber security.	1. Familiarize with cyber security concepts. 2. Check security of various sites in Internet. 3. Check cookie settings on a computer. 4. Familiarize with HTTP and HTTPS protocols. 5. Perform mapping and port settings. 6. Check browser security settings on a computer/ mobile/ tab etc. 7. Check email security. 8. Set strong passwords. 9. Change passwords periodically 10. Use password vaults to store passwords i.e., Bitwarden, Dashlane, Zoho vault. 11. Create hash value of a document with open source/ freeware hash creating tool.	• Cyber security concepts. • Dark Web concepts. • Introduction to cloud security. • Digital Forensics and FTK imaging. • HTTP and HTTPS. • SSL. • Firewall. • Password setting techniques. • Password changing. • Password vaults.
Professional skills 35 Hrs. Professional Knowledge- 10 Hrs.	Lo-2: Familiarization to recent cyber-crime incidents and related Laws to protect.	12. Familiarize with cyber-attack events in near past. 13. Familiarize with the types of cyber security attacks. 14. Familiarize with the cyber laws of Govt. of India. 15. Familiarize with the cyber portal of govt. of India to report cyber-crime.	• Introduce to various types of cyber-attacks, i.e., Phishing, catfishing, Cyber Stalking, Cyber Bullying. • Ransomware, Social Engg. attacks, Insider theft, identity theft, Sextortion, YouTube Like

		16. Report to Police Station in case of cyber-attacks. 17. Visit various cyber-crime portals.	and Subscribe Scam, advertising related fraud. • Other types of frauds i.e., QR Code, SMS, Job, KYC, remote Access, dating, Aadhaar Enabled Payment System. • Impersonation, customer care fraud, Loan app, Sim swap, vishing, smishing, Shoulder Surfing, baiting, spear fishing, whaling, tailgating/piggybacking. • Cyber Crimes and Legal Framework. • Cyber-crime reporting portal to report cyber-crime cases - www.cybercrime.gov. in. • Helpline number 1930. • Indian Cyber Crime Coordination Centre. • National Cyber Forensic Lab. • CyTrain portal.
Professional skills 10 Hrs. Professional Knowledge 05 Hrs.	LO-3: Perform vulnerability assessments on sample systems.	18. Perform Port Scanning using TCP Port Scanner, Nmap, Netcat. 19. Conduct Risk Identification and Analysis. 20. Vulnerability Scanning Policies and Procedures. 21. Demonstrate penetration testing using tools such as Nmap, Metasploit, Wireshark	• Vulnerability Assessment • Types of scans • Penetration Testing
Professional skills 10 Hrs. Professional	LO-4: Familiarize to different security control mechanisms.	22. Familiarize with safeguarding financial transitions.	• Safeguarding financial transactions. • Debit/credit card limit.

Knowledge 05 Hrs.		23. Follow safe browsing techniques. 24. Perform Biometric lock/unlock. 25. Identify fake websites.	• Internet banking safeguard • Reporting fraud. • Password protocols. • Aadhaar Enabled Payment System. • Locking Biometrics in UIDAI. • Identify fake websites. • Malware and its types. • Effects of malware attacks on computer. • Protection from Malware i.e., using original OS, Backup of data in regular intervals, Updating OS, Anti-Virus.
Professional skills 10 Hrs. Professional Knowledge 05 Hrs.	LO-5: Perform cyber-attack simulations.	26. Perform role play of cyberattack phone calls. 27. Demonstrate how cybercrime happens, like: smshing, vishing, email phishing etc.	• Cyberattacks simulation.
Professional skills 10 Hrs. Professional Knowledge 05 Hrs.	LO-6: Implement encryption techniques on sample data and analyze the results.	28. Perform encryption and decryption operation on sample data.	• Encryption and decryption techniques using symmetric and asymmetric cryptography.
Professional skills 10 Hrs. Professional Knowledge 05 Hrs.	LO-7: Set up and configure firewalls and intrusion detection systems.	29. Install intrusion detection system i.e., suricata/ solarwinds. 30. Install intrusion detection system in Linux using snort. 31. Turn on / turn off Windows defender firewall. 32. Install Firewall in Linux.	• Concept of Firewall and intrusion detection systems. •
Professional skills 10 Hrs.	LO-8: Familiarize with Social Engineering	33. SOPs/ dos and don'ts for social media user.	• Overview of Social Engineering attacks.

Professional Knowledge 05 Hrs.	attacks	34. Role play social engineering attacks.	• Types of attacks. • Guidelines of preventive measures from social engineering attack.
Professional skills 40 Hrs. Professional Knowledge 05 Hrs.	LO-9: Familiarize with ethical hacking.	35. Demonstrate Web Application hacking activity on a sample server. 36. Demonstrate Password hacking activity on sample server. 37. Use Net Surveyor to discover wireless networks.	• Ethical hacking. • Benefits of Ethical Hacking. • Types of Ethical hacking i.e., Web Application, System, Web Server, Wireless Network, Social Engineering. • Phases of Ethical Hacking. • Denial of Service (DoS). • Rogue Access Points. • MAC spoofing. • Man-in-the-middle.
Professional skills 10 Hrs. Professional Knowledge 05 Hrs.	LO-10: Perform network traffic analysis and identify potential threats.	38. Show vulnerability of RDP (Remote Desktop protocol). 39. Demonstrate unencrypted management protocols, such as: telnet, Http, SNMP.	**Network Traffic Analysis (NTA)** • Key benefits of NTA Purpose of Monitoring Network Traffic
Professional skills 10 Hrs. Professional Knowledge 05 Hrs.	LO-11: Simulate incident response scenarios and develop incident response plans.	40. Perform protect, detect and response from malware, phishing, Ransomware.	**Incident Response Scenarios** • Observe, Orient, Decide, and Act (OODA) loop. • PDR (protect, Detect, Response).

6. ASSESSMENT CRITERIA

LEARNING OUTCOME	ASSESSMENTCRITERIA
1. Familiarize with fundamentals of cyber security.	Identify https sites and http sites
	Set browser security
	Demonstrate how to set strong password
	Demonstrate using password vaults
2. Familiarize to recent cybercrime incidents and related Laws to protect.	Open cyber-crime portal of Govt. of India
	Describe different types of cyber-attack incidents
	Set browser security
	Set email security
3. Perform vulnerability assessments on sample systems.	Perform port scanning using tools
	Perform Network scanning using tools
	Create vulnerability assessment plan
4. Familiarize to different security control mechanisms.	Set biometric lock / unlock using Uidai site.
	Describe steps to protect computer from Malware
	Perform backup of data
	Update OS.
5. Perform cyber-attack simulations.	Describe how cyber-attacks happen
6. Implement encryption techniques on sample data and analyze the results.	Perform RSA encryption on sample data using online tools.
7. Set up and configure firewalls and intrusion detection systems.	Install IDS on Windows computer
	Install IDS on Linux computer
	Install firewall in Linux
8. Familiarize with Social Engineering attacks.	Describe different types of cyberattack incidents using social engineering and how to avoid.
9. Familiarize with ethical hacking.	Perform web application hacking activity on a sample server.
	Perform password hacking activity on a sample server.
	Discover wifi networks using tools
	Perform hacking WPA network.
10. Perform network traffic	Demonstrate ransomware attacks on a sample server
	Demonstrate unencrypted management protocols, such as: telnet,

analysis and identify potential threats.	Http, SNMP
	Perform Network monitoring using various tools
11. Simulate incident response scenarios and develop incident response plans.	Perform incident response from malware, phishing, Ransomware.

ANNEXURE-I

LIST OF TOOLS & EQUIPMENT			
S No.	**Name of the Tools and Equipment**	**Specification**	**Quantity**
Same as COPA / IT / CHNM / ICTSM / DBSA / DTPO / MASE under CTS OR CSA / CHNM / IT / DTPO under CITS.			
Additional Tools & Equipment required			
1.	Network monitoring tools such as Solar Winds or similar	Preferably open source	As required
2.	Open source FTK tool and hash value creation tool	Preferably open source	As required
3.	Network monitoring tools such as EnCash/nagios/zabbis/solarwinds or similar	Preferably open source	As required
4.	Penetration testing tools such as Nmap, Metasploit, Wireshark,	Preferably open source	As required
5.	NetSurveyor or similar	Preferably open source	As required
6.	Intrusion detection system i.e., Solarwinds, suricate,	Preferably open source	As required
7.	password vaults to store passwords i.e., Bitwarden, Dashlane, Zoho vault or similar opensource tool to check password matrix	Preferably open source	As required
8.	Port Scanner or similar	Preferably open source	As required
9.	NMap or similar	Preferably open source	As required
10.	Netcat or similar	Preferably open source	As required
11.	MiTeC or similar	Preferably open source	As required
12.	NetScanTools or similar	Preferably open source	As required
13.	Bitwarden or similar	Preferably open source	As required
14.	Dashlane or similar	Preferably open source	As required
15.	Zoho vault or similar	Preferably open source	As required

ANNEXURE-II

The DGT sincerely acknowledges contributions of the Industries, State Directorates, Trade Experts, Domain Experts and all others who contributed in designing/ revising the curriculum. Special acknowledgement is extended by DGT to the following expert members who had contributed immensely in this curriculum.

List of members attended the Trade Committee Meeting for designing of BASICS OF Cyber Security syllabus under Short Term Courses held on 21st March, 2024 at CSTARI, Kolkata.

Sl. No.	Name and Designation (Shri/Smt./Kumari)	Organization with Address	Remarks
1.	Sunil Kumar Gupta, DDG (ER)	CSTARI, Kolkata	Chairman
2.	G.C. Saha, Jt. Director/HoD	CSTARI, Kolkata	Member
3.	Rama Nandi, Associate Manager	Accenture, Unitech Kolkata	Member
4.	Asok Bandyopadhyay, Scientist F, Head ICT&S Group	C-DAC, Kolkata	Member
5.	Amlan Raychaudhuri, Asst. Professor	BP Poddar Institute of Management & Technology, Kolkata	Member
6.	Niladri Roy, Enterprise Architect	TCS, Kolkata, Ecospace	Member
7.	Avishek Paul, Asst. Professor	Techno India Group, Kolkata	Member
8.	Diptadip Maiti, Asst. Professor	Techno College of Engineering, Agartala	Member
9.	Amit Kumar Mondal, Asst. Professor	Bengal Institute of Technology (A unit of Techno India Group), Kolkata	Member
10.	Anindya Sundar Das Gupta	Women ITI, Banipur	Member
11.	Subhendu Chakrabarty, Technical Expert	CSCOE, DITE, WB	Member
12.	P. Suresh, Sr. Executive	Vi Micro Systems Private Limited, Chennai	Member
13.	Goutam Roy	Prime Infoserv LLP	Member
14.	Brindaban Das, Dy. Director	CSTARI, Kolkata	Member
15.	Murari Barui, Asst. Director	CSTARI, Kolkata	Member
16.	Sk. Altaf Hossain, Asst. Director	CSTARI, Kolkata	Member
17.	Akhilesh Pandey, Asst. Director	CSTARI, Kolkata	Member
18.	Bhagat Singh, Asst. Director	CSTARI, Kolkata	Member

19.	Manish Mishra, Asst. Director	NSTI, Howrah	Member
20.	P.K. Bairagi, TO	CSTARI, Kolkata	Member
21.	B. Biswas, TO	CSTARI, Kolkata	Member
22.	K.V.S. Narayana, TO	CSTARI, Kolkata	Member
23.	Swapan Sen, TO	CSTARI, Kolkata	Member
24.	Pradip Biswas, Jr. D/man	CSTARI, Kolkata	Member
25.	Hemant Kujur, Jr. D/man	CSTARI, Kolkata	Member
26.	Jinendran PK, JC	CSTARI, Kolkata	Member