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

COMPETENCY BASED CURRICULUM

CYBER SECURITY ASSISTANT

(Duration: One year)

CRAFTSMEN TRAINING SCHEME (CTS)

NSQF LEVEL- 3.5

SECTOR –IT & ITES

Directorate General of Training

CYBER SECURITY ASSISTANT

(Non-Engineering Trade)

(Designed in August 2023)

Version: 1.0

CRAFTSMEN TRAINING SCHEME (CTS)

NSQF LEVEL – 3.5

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
www.cstaricalcutta.gov.in

CONTENTS

1. COURSE INFORMATION

During the one-year duration of Cyber Security Assistant trade a candidate is trained on professional skill, professional knowledge and Employability skill related to job role. In addition to this a candidate is entrusted to undertake project work and extracurricular activities to build up confidence. The broad components covered under Professional skill subject are as below:-

At the beginning of the training program, trainees will focus on learning the implementation of safe working practices, adhering to environmental regulations, and maintaining good housekeeping. As they progress, they will acquire fundamental knowledge and skills related to computers, including their components and common software applications, all while emphasizing safety in PC use. Additionally, trainees will gain an understanding of computer networks, including their components, protocols, and basic network administration. They will also delve into essential aspects of operating systems and security concepts. Furthermore, trainees will learn to interpret principles, practices, and methodologies for web application security, ensuring organizations are safeguarded from potential threats. Ethical hacking will be a significant part of their training, enabling them to identify and address security vulnerabilities in computer systems, networks, and applications. They will also develop the ability to recognize, assess, and mitigate security risks and vulnerabilities in software applications. Additionally, trainees will acquire skills to identify social engineering attempts and implement strategies for defense against such attacks. They will also gain insights into the security challenges associated with wireless networks and methods to assess and secure them effectively. Towards the end of their training, trainees will be well-equipped to respond to cybersecurity incidents and preserve digital evidence, rounding out their comprehensive cybersecurity skillset.

2. TRAINING SYSTEM

2.1 GENERAL

The Directorate General of Training (DGT) under Ministry of Skill Development & Entrepreneurship offers a range of vocational training courses catering to the need of different sectors of economy/ Labour market. The vocational training programmes are delivered under the aegis of Directorate General of Training (DGT). Craftsman Training Scheme (CTS) with variants and Apprenticeship Training Scheme (ATS) are two pioneer schemes of DGT for strengthening vocational training.

Cyber Security Assistant trade under CTS is one of the newly designed courses. The CTS courses are delivered nationwide through network of ITIs. The course is of one-year duration. It mainly consists of Domain area and Core area. In the Domain area (Trade Theory & Practical) impart professional skills and knowledge, while Core area (Employability Skills) imparts requisite core skill, knowledge and life skills. After passing out the training program, the trainee is awarded National Trade Certificate (NTC) by DGTwhich is recognized worldwide.

Trainee needs to demonstrate broadly that they are able to:

- Read and interpret technical parameters/ documentation, plan and organize work processes, identify necessary materials and tools;
- Perform task with due consideration to safety rules, accident prevention regulations and environmental protection stipulations;
- Apply professional knowledge & employability skills while performing the job and repair & maintenance work.
- Document the technical parameter related to the task undertaken.

2.2 PROGRESSION PATHWAYS

- Can join industry as Cyber Security Assistant and will progress further as Security Analyst, Cyber Security Team Lead and can rise to the level of Cyber Security Manager.
- Can become Entrepreneur in the related field.
- Can join Apprenticeship programme in different types of industries leading to National Apprenticeship certificate (NAC).
- Can join Crafts Instructor Training Scheme (CITS) in the trade for becoming instructor in ITIs.
- Can join Advanced Diploma (Vocational) courses under DGT as applicable.

2.3 COURSE STRUCTURE

Table below depicts the distribution of training hours across various course elements during a period of one year:

S No.	Course Element	Notional Training Hours
1	Professional Skill (Trade Practical)	840
2	Professional Knowledge (Trade Theory)	240
3	Employability Skills	120
	Total	**1200**

Every year 150 hours of mandatory OJT (On the Job Training) at nearby industry, wherever not available then group project is mandatory.

4	On the Job Training (OJT)/ Group Project	150
5	Optional Courses (10th/ 12th class certificate along with ITI certification or add on short term courses)	240

Trainees of one-year or two-year trade can also opt for optional courses of up to 240 hours in each year for 10th/ 12th class certificate along with ITI certification, or, add on short term courses.

2.4 ASSESSMENT & CERTIFICATION

The trainee will be tested for his skill, knowledge and attitude during the period of course through formative assessment and at the end of the training programme through summative assessment as notified by the DGT from time to time.

a) The **Continuous Assessment** (Internal) during the period of training will be done by **Formative Assessment Method** by testing for assessment criteria listed against learning outcomes. The training institute has to maintain an individual trainee portfolio as detailed in assessment guideline. The marks of internal assessment will be as per the formative assessment template provided on www.bharatskills.gov.in

b) The final assessment will be in the form of summative assessment. The All India Trade Test for awarding NTC will be conducted by Controller of examinations, DGT as per the guidelines. The pattern and marking structure are being notified by DGT from time to time. **The learning outcome and assessment criteria will be the basis for setting question papers for final**

assessment. The examiner during final examination will also check the individual trainee's profile as detailed in assessment guideline before giving marks for practical examination.

2.4.1 PASS REGULATION

For the purposes of determining the overall result, weightage of 100 % is applied for six months and one-year duration courses and 50% weightage is applied to each examination for two years courses. The minimum pass percent for Trade Practical and Formative assessment is 60% & for all other subjects is 33%.

2.4.2 ASSESSMENT GUIDELINE

Appropriate arrangements should be made to ensure that there will be no artificial barriers to assessment. The nature of special needs should be taken into account while undertaking assessment. Due consideration should be given while assessing for teamwork, avoidance/reduction of scrap/wastage and disposal of scarp/wastage as per procedure, behavioral attitude, sensitivity to environment and regularity in training. The sensitivity towards OSHE and self-learning attitude are to be considered while assessing competency.

Assessment will be evidence based comprising some of the following:

- Job carried out in labs/workshop
- Record book/ daily diary
- Answer sheet of assessment
- Viva-voce
- Progress chart
- Attendance and punctuality
- Assignment
- Project work
- Computer based multiple choice question examination
- Practical Examination

Evidences and records of internal (Formative) assessments are to be preserved until forthcoming examination for audit and verification by examination body. The following marking pattern to be adopted for formative assessment:

Performance Level	Evidence
(a) Marks in the range of 60 -75% to be allotted during assessment	
For performance in this grade, the candidate with occasional guidance and showing due regard for safety procedures and practices, has produced work which demonstrates attainment	• Demonstration of good skill in the use of hand tools, machine tools and workshop equipment • 60-70% accuracy achieved while

of an acceptable standard of craftsmanship.	undertaking different work with those demanded by the component/job/set standards. • A fairly good level of neatness and consistency in the finish • Occasional support in completing the project/job.
(b)Marks in the range of above75% - 90% to be allotted during assessment	
For this grade, the candidate, with little guidance and showing due regard for safety procedures and practices, has produced work which demonstrates attainment of a reasonable standard of craftsmanship.	• Good skill levels in the use of hand tools, machine tools and workshop equipment • 70-80% accuracy achieved while undertaking different work with those demanded by the component/job/set standards. • A good level of neatness and consistency in the finish • Little support in completing the project/job
(c) Marks in the range of above 90% to be allotted during assessment	
For performance in this grade, the candidate, with minimal or no support in organization and execution and with due regard for safety procedures and practices, has produced work which demonstrates attainment of a high standard of craftsmanship.	• High skill levels in the use of hand tools, machine tools and workshop equipment • Above 80% accuracy achieved while undertaking different work with those demanded by the component/job/set standards. • A high level of neatness and consistency in the finish. • Minimal or no support in completing the project.

3. JOB ROLE

Brief description of job role:

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

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 authorisation 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. Sends printouts listing employee data authorisation to computer user departments to verify or correct information in security files. Reviews data use records and compares user names listed in records with employee authorisation to ensure that all employees who accessed data files were entitled to do so. Deletes data access of unauthorised users, and for users who have not used data for specified time.

Computer Network Professionals, Other Covers computing professionals not classified elsewhere in Group 213, Computing Professionals.

Reference NCO-2015:

a) 2522.0201 – Security Analyst
b) 3513.0200 – Computer Security Specialist
c) 2523.9900 – Computer Network Professionals, Other

Reference NOS:

i. CSC/N9501,
ii. CSC/N9502,
iii. CSC/N9503,
iv. CSC/N9504,
v. CSC/N9505**,**
vi. CSC/N9506,
vii. CSC/N9507,
viii. CSC/N9508,
ix. CSC/N9509,
x. CSC/N9510

4. GENERAL INFORMATION

Name of the Trade	**CYBER SECURITY ASSISTANT**
Trade Code	TBD
NCO – 2015	2522.0201, 3513.0200, 2523.9900
NOS covered	CSC/N9501, CSC/N9502, CSC/N9503, CSC/N9504, CSC/N9505, CSC/N9506, CSC/N9507, CSC/N9508, CSC/N9509, CSC/N9510
NSQF Level	Level-3.5
Duration of Craftsmen Training	One year (1200 hours + 150 hours OJT/Group Project)
Entry Qualification	10th Class Passed
Minimum Age	18 years as on first day of academic session.
Eligibility for PwD	LD, LC, DW, AA, LV, DEAF, AUTISM, SLD
Unit Strength (No. Of Student)	24 (There is no separate provision of supernumerary seats)
Space Norms	70 Sq. m
Power Norms	3.45 KW
Instructors Qualification for	
(i) Cyber Security Assistant Trade	B.Voc/Degree in Computer Science/Computer Application/ Information Technology from AICTE/UGC recognized College/ university with one-year experience in the relevant field. **OR** Diploma (Minimum 2 years) in Computer Science/ Computer Application/ Information Technology from AICTE/recognized board of technical education or relevant Advanced Diploma (Vocational) from DGT with two years' experience in the relevant field. **OR** NTC/NAC passed in the Trade of "Cyber Security Assistant" With three years' experience in the relevant field. **<u>Essential Qualification:</u>** Relevant Regular / RPL variants of National Craft Instructor Certificate (NCIC) under DGT. **Note: - Out of two Instructors required for the unit of 2 (1+1), one must have Degree/Diploma and other must have NTC/NAC qualifications. However. both of them must possess NCIC in any of its variants.**
(ii) Employability Skill	MBA/ BBA / Any Graduate/ Diploma in any discipline with Two

	years' experience with short term ToT Course in Employability Skills. (Must have studied English/ Communication Skills and Basic Computer at 12th / Diploma level and above) OR Existing Social Studies Instructors in ITIs with short term ToT Course in Employability Skills.
(iii) Minimum Age for Instructor	21 Years
List of Tools & Equipment	As per Annexure-I

5. LEARNING OUTCOME

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

5.1 LEARNING OUTCOME

1. Demonstrate implementation of safe working practices, environment regulation, and housekeeping. (NOS: CSC/N9501)
2. Acquire fundamental knowledge and skills related to computers, their components, and common software applications and safety related to PC. (NOS: CSC/N9502)
3. Interpret computer networks, their components, protocols, and basic network administration. (NOS: CSC/N9503)
4. Identify essential aspects of operating systems and security concepts. (NOS: CSC/N9504)
5. Interpret Web Application Security principles, practices, and methodologies to protect organizations from potential threats**.** (NOS: CSC/N9505)
6. Identify and address security vulnerabilities in computer systems, networks, and applications by ethical hacking. (NOS: CSC/N9506)
7. Identify, assess, and mitigate security risks and vulnerabilities in software applications. (NOS: CSC/N9507)
8. Recognize social engineering attempts, and implement effective strategies to defend against social engineering attacks. (NOS: CSC/N9508)
9. Identify security challenges of wireless networks and the methodologies used to assess and secure them. (NOS: CSC/N9509)
10. Respond to cyber security incidents and preserve digital evidence. (NOS: CSC/N9510)

6. ASSESSMENT CRITERIA

LEARNING OUTCOMES	ASSESSMENT CRITERIA
1. Demonstrate implementation of safe working practices, environment regulation, and housekeeping. (NOS: CSC/N9501)	Demonstrate safety precaution including anti- static protection.
	Demonstrate first aid practice.
	Demonstrate artificial respiration and practice.
	Demonstrate electrical safety precautions.
2. Acquire fundamental knowledge and skills related to computers, their components, and common software applications and safety related to PC. (NOS: CSC/N9502)	Demonstrate specification and application of basic hand tools.
	Create New Document and save document.
	Demonstrate text formatting, paragraph formatting, Perform page setup.
	Insert image, header & footer, page number, tables etc.
	Demonstrate spells check and grammar/ page breaks/ printing.
	Perform mail merge.
	Opening Excel and apply Basic Formulas/ AutoFill/ Formatting Cells/ Working with Functions/ Charts and Graphs/ Sorting and Filtering Data/ Freezing Panes.
	Create New Presentation using MS power point.
	use Search Engines, Navigate Websites, use Hyperlinks.
	Create email, social media accounts e.g. Twitter, LinkedIn etc.
	Demonstrate Downloading and Uploading.
	Connect device to the internet by selecting an available network - wired (e.g., Ethernet) or wireless (e.g., Wi-Fi) and entering the required credentials.
3. Interpret computer networks, their components, protocols, and basic network administration. (NOS: CSC/N9503)	Identify types of Networks.
	Explore TCP/IP (Ver. 4 & Ver. 6) Models and OSI Layers.
	Set up a physical lab to practice routing and switching.
	Set up a simple network with two routers and two switches and ensure they can communicate with each other.
	Configure static routes on routers to allow communication between multiple networks.
	Set up dynamic routing protocols like OSPF (Open Shortest Path First) or EIGRP (Enhanced Interior Gateway Routing Protocol) to automatically exchange routing information between routers.
	Create and configure VLANs on switches, and enable inter-VLAN communication.

	Configure STP to prevent network loops in redundant switch topologies.
	Practice implementing ACLs to control traffic flow based on specific criteria.
4. Identify essential aspects of operating systems and security concepts. (NOS: CSC/N9504)	Install HyperVisor
	Create VMs using HyperVisor.
	Create virtual versions of computing resources, such as operating systems/ servers/ storage devices/ networks to allow multiple virtual machines (VMs) to run on a single physical machine, effectively sharing resources.
	Demonstrate authentication/ access control/ encryption/ network security/ and common security threats for securing both Windows and Linux systems from potential cyber threats.
	Interpret cloud computing deployment models (public, private, hybrid, and multi-cloud), service models (IaaS, PaaS, SaaS), and the benefits and challenges of adopting cloud technologies.
	Demonstrate the core services and features offered by AWS/Azure/GCP.
5. Interpret Web Application Security principles, practices, and methodologies to protect organizations from potential threats. (NOS: CSC/N9505)	Use HTTP (Hypertext Transfer Protocol) for communication between web browsers and servers.
	Data transmission using HTTPS (HTTP Secure) which adds layer of security using TLS/SSL (Transport Layer Security/Secure Sockets Layer) encryption to protect data during transmission.
	Identify potential security concerns related to Cookies.
	Use tokens to authenticate and authorize web applications for secure user identification and validation.
	Use cryptography encryption algorithms/ hashing/digital signatures for encoding and decoding information to protect its confidentiality, integrity, and authenticity.
	Vulnerability Calculation NIST framework OWASP TOP10 FRAMEWORK.
	Secure communication and encryption on the internet using Public Key Infrastructure (PKI).
	Secure email communication to prevent unauthorized access to the content of messages using PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Mail Extensions).
	Practice methods of attacking and analyzing cryptographic algorithms.

	Identify and apply online tracking methods, including cookies and other tracking technologies.
	Apply best practices for secure application configurations to prevent Security Misconfiguration.
	Test for Vulnerable and Outdated Components to identify potential security risks and apply necessary updates.
	Identify Common authentication vulnerabilities, such as weak passwords, session management issues, and multi-factor authentication.
6. Identify and address security vulnerabilities in computer systems, networks, and applications by ethical hacking. (NOS: CSC/N9506)	Use the Cyber Kill Chain framework to identify and mitigate potential threats.
	Perform Information gathering for collecting data about the target system or network.
	Apply Scanning process for actively probing the target to identify potential vulnerabilities and open ports.
	Perform Footprinting through web services and public information/ Social Networking Sites /Website/ Email/ WHOIS.
	Perform host discovery to identify active hosts on a network using various methods like ping sweeps and port scanning.
	Perform Port and Service Discovery by applying techniques for identifying open ports and services running on the target system to understand potential points of attack.
	Assess potential vulnerabilities in target systems to understand the security weaknesses that could be exploited.
	Use network sniffing to analyze the data flow and identify security vulnerabilities.
	Use spoofing, forging or faking data, such as IP addresses, to disguise the source of network packets.
	Perform Network and system exploitation by utilizing the identified vulnerabilities to gain unauthorized access or control over target systems.
	Apply Privilege escalation process for gaining higher levels of access and permissions on a system beyond what the initial compromise provided.
7. Identify, assess, and mitigate security risks and vulnerabilities in software applications. (NOS:	Perform Application penetration testing by assessing the security of an application by actively simulating real-world attacks.
	Elimination of false positive from tool output.

CSC/N9507)	Attempt to exploit vulnerabilities in the application to understand potential risks and recommend mitigation strategies.
	Perform Authentication Testing by applying techniques to assess the effectiveness of authentication mechanisms and identify vulnerabilities like weak passwords, brute-force attacks, or credential stuffing.
	Analyze authorization mechanisms to ensure that unauthorized users cannot access sensitive data or perform restricted operations.
	Explore techniques like Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and other attacks that exploit vulnerabilities in the client-side code.
	Prevent server-side attacks by SQL injection, remote code execution, and server misconfigurations.
	Perform Network Penetration Testing by network vulnerability scanning, identifying open ports, and assessing network security configurations.
	Perform Mobile Application Penetration Testing.
8. Recognize social engineering attempts, and implement effective strategies to defend against social engineering attacks. (NOS: CSC/N9508)	Apply various social engineering techniques such as pretexting, baiting, tailgating, and quid pro quo.
	Prevent Phishing & Vishing attacks and recommend measures.
	Demonstrate how social engineering can be used to exploit insiders for malicious purposes.
	Identify techniques used by attackers to conduct identity theft and how to protect against it.
9. Identify security challenges of wireless networks and the methodologies used to assess and secure them. (NOS: CSC/N9509)	Identify different wireless standards (e.g., Wi-Fi 802.11)/ frequency bands/ wireless modes (ad-hoc, infrastructure)/ and wireless network architectures.
	Interpret potential threats to wireless networks such as eavesdropping/ unauthorized access/ rogue access points/ denial-of-service (DoS) attacks/ man-in-the-middle (MITM) attacks and prevention & mitigation.
	Apply Steps for Wireless Hacking Methodology involved in assessing the security of wireless networks, from reconnaissance to exploitation.
	Identify and use Various wireless network penetration testing tools like Aircrack-ng, Wireshark, and other utilities for wireless

	assessment and exploitation.
	Practice Bluetooth Hacking considering security aspects of Bluetooth and potential vulnerabilities.
	Identify and use tools specifically designed to secure wireless networks and mitigate threats.
10. Respond to cyber security incidents and preserve digital evidence. (NOS: CSC/N9510)	Provide critical support for identifying, protecting, and remediating dangers such as: Malware, Ransomware, Breaches, Insider threats, Supply chain attacks, Phishing, Denial of service attacks, Cyber-espionage.
	Perform Network monitoring and incident detection.
	Perform Incident management
	Perform Problem management.
	Perform Endpoint administration.
	Perform Security system administration.

SYLLABUS FOR CYBER SECURITY ASSISTANT TRADE			
DURATION: ONE YEAR			
Duration	**Reference Learning Outcome**	**Professional Skills (Trade Practical) With Indicative Hours**	**Professional Knowledge (Trade Theory)**
Professional Skill 20 Hrs.; Professional Knowledge 10 Hrs.	Demonstrate implementation of safe working practices, environment regulation, and housekeeping.	**Familiarization with the Institute and Safety** 1. Visits to workshops, labs, office, stores etc. of the institute. 2. Demonstrate safety precaution including anti-static protection. 3. Demonstrate first aid practice. 4. Demonstrate artificial respiration and practice. 5. Demonstrate electrical safety precautions.	**Familiarization with the Institute and Safety** • Course duration, scope, methodology and structure of the training program. • Safety in moving and shifting heavy and delicate equipments. • First aid concept. • About artificial respiration. • Electrical Safety.
Professional Skill 90 Hrs.; Professional Knowledge 30 Hrs.	Acquire fundamental knowledge and skills related to computers, their components, and common software applications and safety related to PC.	**Computers and their Components** 6. Important Safety Basics. 7. Identification, specification and application of basic hand tools. 8. How to handle components to ensure their longevity. 9. What one shouldn't wear while working inside a computer lab. 10. The danger of static electricity. 11. How to protect a PC from lightning strikes and power outages. 12. Explore windows user interface, file management,	**Computers and their Components** • Computer Hardware Architecture • Introduction to computers, classification, generations, applications. Basic blocks of a digital computer. Hand Tools Basics and Specifications. • Computer Operating System- Microsoft (MS) Windows, Linux Operating System. • Introduction to Word features, Office button, toolbars. • Creating, saving and

		system settings, and administrative tasks. 13. Practice LINUX file system navigation, command-line operations, user management, and basic shell scripting. **Software Applications:** **MS Word** 14. Create New Document and save document. 15. Practice basic text formatting, paragraph formatting, Perform page setup. 16. Insert image, header & footer, page number, tables etc. 17. Practice spells check and grammar, page breaks, printing. 18. Practice mail merge. **MS Excel** 19. Opening Excel and Creating a New Workbook, Saving and Printing, Entering Data, Basic Formulas, AutoFill, Formatting Cells, Working with Functions, Charts and Graphs, Sorting and Filtering Data, Freezing Panes, **MS PowerPoint** 20. Opening PowerPoint and Creating New Presentation. 21. Add Slides, Entering Text, Formatting Text, Adding Images and Media, Slide Design and Themes, Transitions, Animations, Saving and Presenting. **Internet** 22. Identify Web Browsers, use	formatting and printing documents using Word. • Introduction to Excel features, data types and various functions in all categories of Excel. • Concepts of sorting, filtering and validating data. • Introduction to Power Point Slide Show creation process. • Fine tuning the presentation and good presentation technique. • Antivirus

		Search Engines, Navigate Websites, use Hyperlinks 23. Create email, social media accounts e.g. Twitter, LinkedIn etc. 24. Practice Downloading and Uploading. 25. Connect device to the internet by selecting an available network - wired (e.g., Ethernet) or wireless (e.g., Wi-Fi) and entering the required credentials. 26. Antivirus	
Professional Skill 90 Hrs. Professional Knowledge 30 Hrs.	Interpret computer networks, their components, protocols, and basic network administration.	**Networking Fundamentals** 27. Interpret Networking Topology. 28. Identify types of Networks. 29. Explore TCP/IP (Ver. 4 & Ver. 6) Models and OSI Layers. 30. Set up a physical lab to practice routing and switching. 31. Set up a simple network with two routers and two switches and ensure they can communicate with each other. 32. Configure static routes on routers to allow communication between multiple networks. 33. Set up dynamic routing protocols like OSPF (Open Shortest Path First) or EIGRP (Enhanced Interior Gateway Routing Protocol) to automatically exchange routing information between routers. 34. Create and configure VLANs	• Networking Topology and Types of Networks • TCP/IP Models,UDP (Ver. 4 & Ver.6) and OSI Layers • Routing and Switching • Static Routing • Dynamic Routing • VLAN • ACL • NAT • VPN • DHCP • DNS • POP3 • SMTP • SNMP

		on switches, and enable inter-VLAN communication. 35. Configure STP to prevent network loops in redundant switch topologies. 36. Practice implementing ACLs to control traffic flow based on specific criteria.	
Professional Skill 90 hrs. Professional knowledge 30 hrs.	Identify essential aspects of operating systems and security concepts.	**Operating System & Security** Virtualisation 37. Install HyperVisor 38. Create VMs using HyperVisor. 39. Cloud Security 40. Create virtual versions of computing resources, such as operating systems, servers, storage devices, or networks to allow multiple virtual machines (VMs) to run on a single physical machine, effectively sharing resources. 41. Practice Operating Systems and OS Process & Resource Management Security 42. Practice authentication, access control, encryption, network security, and common security threats for securing both Windows and Linux systems from potential cyber threats. 43. Interpret fundamentals of cloud computing. 44. Interpret and Explore cloud computing deployment models (public, private, hybrid, and multi-cloud), service models (IaaS, PaaS, SaaS), and the benefits and	• Virtualisation, Operating Systems and OS Process & Resource Management • HyperVisor • Basic concept of cloud security.

		challenges of adopting cloud technologies. 45. Learn about the essential components that form a cloud infrastructure, such as virtualization, storage, networking, and identity management. 46. Explore the core services and features offered by AWS/Azure/GCP. 47. Secure cloud architecture, focusing on designing and implementing security measures from the ground up considering security at every layer of the cloud infrastructure.	
Professional Skill 100 hrs. Professional knowledge 20 hrs.	Interpret Web Application Security principles, practices, and methodologies to protect organizations from potential threats**.**	**Web Application Security** 48. Interpret and explore IP addresses, domain names, client-server architecture, and the basics of web protocols. 49. Use HTTP (Hypertext Transfer Protocol) for communication between web browsers and servers. 50. Practice data transmission using HTTPS (HTTP Secure) which adds layer of security using TLS/SSL (Transport Layer Security/Secure Sockets Layer) encryption to protect data during transmission. 51. Identify potential security concerns related to Cookies. 52. Interpret sessions for managing user data securely during their interaction with web applications. 53. Use tokens to authenticate	• Basic of Internet and Web Applications, HTTP Protocol, HTTPS - TLS/SSL, how cookies are used, their purpose, and potential security concerns related to them. Sessions, Tokens. Cryptography basics. • Email Encryption, Disk Encryption, Cryptanalysis, Tracking and Privacy, Laws and Compliance.

		and authorize web applications for secure user identification and validation. 54. Use cryptography encryption algorithms, hashing, and digital signatures for encoding and decoding information to protect its confidentiality, integrity, and authenticity. 55. Vulnerability Calculation NIST framework OWASP TOP10 FRAMEWORK. 56. Secure communication and encryption on the internet using Public Key Infrastructure (PKI). 57. Secure email communication to prevent unauthorized access to the content of messages using PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Mail Extensions). 58. Practice methods of attacking and analyzing cryptographic algorithms. 59. Identify and apply online tracking methods, including cookies and other tracking technologies. 60. Discuss privacy concerns and measures to safeguard personal information. 61. Interpret laws related to information security, data protection, and compliance. 62. Apply best practices for secure application configurations to prevent Security Misconfiguration.	

		63. Test for Vulnerable and Outdated Components to identify potential security risks and apply necessary updates. 64. Identify Common authentication vulnerabilities, such as weak passwords, session management issues, and multi-factor authentication.	
Professional Skill 125 hrs. Professional knowledge 25 hrs.	Identify and address security vulnerabilities in computer systems, networks, and applications by ethical hacking.	**Ethical Hacking** 65. Interpret difference between ethical hacking (authorized penetration testing) and malicious hacking. 66. Interpret and use the Cyber Kill Chain framework to identify and mitigate potential threats. 67. Practice Information gathering for collecting data about the target system or network. 68. Practice Scanning process for actively probing the target to identify potential vulnerabilities and open ports. 69. Perform Footprinting through web services and public information. 70. Perform Footprinting through Social Networking Sites. 71. Perform Website Footprinting. 72. Perform Email Footprinting. 73. Perform WHOIS Footprinting. 74. Perform host discovery to	• Interpret principles, methodologies, and legal aspects of ethical hacking. • Ethical Hacking Introduction • Cyber Kill Chain, Information Gathering and Scanning • Footprinting through Web Services, Footprinting through Social Networking Sites, Website Footprinting, Email Footprinting, WHOIS Footprinting, • Host Discovery, Port and Service Discovery, OS Discovery (Banner Grabbing/OS Fingerprinting), Scanning Beyond IDS and Firewall, Vulnerability Analysis, Weaponisation, Delivery, Sniffing and Spoofing, Network and System Exploitation, Command and Control, Privilege Escalation, Post Exploitation, Steganography.

		identify active hosts on a network using various methods like ping sweeps and port scanning. 75. Perform Port and Service Discovery by applying techniques for identifying open ports and services running on the target system to understand potential points of attack. 76. Assess potential vulnerabilities in target systems to understand the security weaknesses that could be exploited. 77. Use network sniffing to analyze the data flow and identify security vulnerabilities. 78. Use spoofing, forging or faking data, such as IP addresses, to disguise the source of network packets. 79. Perform Network and system exploitation by utilizing the identified vulnerabilities to gain unauthorized access or control over target systems and recommend appropriate security measures. 80. Apply Privilege escalation process for gaining higher levels of access and permissions on a system beyond what the initial compromise provided.	
Professional Skill 100 hrs. Professional	Identify, assess, and mitigate security risks and vulnerabilities in	**Application Security** 81. Perform Application penetration testing by assessing the security of an	• Application Penetration Testing, Authentication Testing, Authorisation Testing, Client Side Attacks,

knowledge 20 hrs.	software applications.	application by actively simulating real-world attacks. 82. Elimination of false positive from tool output. 83. Attempt to exploit vulnerabilities in the application to understand potential risks and recommend mitigation strategies. 84. Perform Authentication Testing by applying techniques to assess the effectiveness of authentication mechanisms and identify vulnerabilities like weak passwords, brute-force attacks, or credential stuffing. 85. Analyze authorization mechanisms to ensure that unauthorized users cannot access sensitive data or perform restricted operations. 86. Explore techniques like Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and other attacks that exploit vulnerabilities in the client-side code. 87. Prevent server-side attacks by SQL injection, remote code execution, and server misconfigurations. 88. Perform Network Penetration Testing by network vulnerability scanning, identifying open ports, and assessing network	Server Side Attacks, Network Penetration Testing, Mobile Application Penetration Testing.

		security configurations. 89. Perform Mobile Application Penetration Testing. 90. Emphasize ethical guidelines, ensuring appropriate legal and ethical practices.	
Professional Skill 45 hrs. Professional knowledge 15 hrs.	Recognize social engineering attempts, and implement effective strategies to defend against social engineering attacks.	**Social Engineering** 91. Explore various social engineering techniques such as pretexting, baiting, tailgating, and quid pro quo used by attackers to trick individuals into divulging sensitive information or taking specific actions. 92. Practice preventing Phishing & Vishing attacks and recommend measures. 93. Explores how social engineering can be used to exploit insiders for malicious purposes. 94. Identify techniques used by attackers to conduct identity theft and how to protect against it.	• Social Engineering Concepts, Social Engineering Techniques, Phishing Attacks, Vishing, Insider Threats, Impersonation on Social Networking Sites, Identity Theft
Professional Skill 90 hrs. Professional knowledge 30 hrs.	Identify security challenges of wireless networks and the methodologies used to assess and secure them.	**Hacking Wireless Network** 95. Identify different wireless standards (e.g., Wi-Fi 802.11), frequency bands, wireless modes (ad-hoc, infrastructure), and wireless network architectures. 96. Interpret potential threats to wireless networks such as eavesdropping, unauthorized access, rogue access points, denial-of-service (DoS) attacks, man-in-the-middle (MITM) attacks and prevention &	• Wireless Concepts, Wireless Encryption, Wireless Threats, Wireless Hacking Methodology, Wireless Hacking Tools, Bluetooth Hacking, Wireless Security Tools.

		mitigation. 97. Apply Steps for Wireless Hacking Methodology involved in assessing the security of wireless networks, from reconnaissance to exploitation. 98. Identify and use Various wireless network penetration testing tools like Aircrack-ng, Wireshark, and other utilities for wireless assessment and exploitation. 99. Practice Bluetooth Hacking considering security aspects of Bluetooth and potential vulnerabilities. 100. Identify and use tools specifically designed to secure wireless networks and mitigate threats.	
Professional Skill 90 hrs. Professional knowledge 30 hrs.	Respond to cyber security incidents and preserve digital evidence.	**SOC (Security Operation Centre) & Incident Response.** 101. Provide critical support for identifying, protecting, and remediating dangers such as: Malware, Ransomware, Breaches, Insider threats, Supply chain attacks, Phishing, Denial of service attacks, Cyber-espionage. 102. Practice Network monitoring and incident detection. 103. Practice Incident management 104. Practice Problem management 105. Practice Endpoint administration. 106. Practice Security system administration	• Continuous proactive monitoring • Alert ranking and management • Threat response • Recovery and remediation • Log management • Root cause investigation • Protective measures in response to incidents • Analysing the aftermath of incidents • Staying up-to-date with the latest cybercrime trends • Creating incident response plans • Patching vulnerabilities
Project Work/Industrial Visit (Optional)			

SYLLABUS FOR CORE SKILLS
1. Employability Skills (Common for all CTS trades) (120hrs.)

Learning outcomes, assessment criteria, syllabus and Tool List of Core Skills subjects which is common for a group of trades, provided separately in www.bharatskills.gov.in/ dgt.gov.in

ANNEXURE-I

List of Tools & Equipment			
Cyber Security Assistant (for batch of 24 Candidates)			
S No.	**Name of the Tools and Equipment**	**Specification**	**Quantity**
A. TRAINEES TOOL KIT			
1.	Connecting screw driver	100 mm	24 Nos.
2.	Neon tester	500 V.	24 Nos.
3.	Screw driver set	(set of 5)	24 Nos.
4.	Insulated combination pliers	150 mm	24 Nos.
5.	Insulated side cutting pliers	150 mm	24 Nos.
6.	Long nose pliers	150mm	24 Nos.
7.	Soldering iron	25W.240V.	24 Nos.
8.	Electrician knife		24 Nos.
9.	Tweezers	100 mm	24 Nos.
10.	Digital Multimeter	4000 Counts, LCD Display 3 ¾ Digital multimeter to test AC/DC Voltage and Current, Resistance, Temperature and Transistor (hhFE) , duty cycle , Diode and Continuity measurement Data Hold.	24 Nos.
11.	Soldering Iron Changeable bits	15W	24 Nos.
12.	De-soldering pump		24 Nos.
B. LIST OF TOOLS			
13.	Crimping tool(pliers)		2 Nos.
14.	Soldering Iron	25W	6 Nos.
15.	Magneto spanner set		2 Nos.
16.	Screwdriver	150mm	4 Nos.
17.	Steel rule	150mm	2 Nos.
18.	Scriber straight	150mm	2 Nos.
19.	Soldering Iron	240W	1 No.
20.	Allen key set	(set of 9)	2 Nos.
21.	Tubular box spanner	(setof6nos.)	1 No.
22.	Magnifying lenses	75mm	3 Nos.
23.	Continuity tester		6 Nos.
24.	Soldering iron	10W	6 Nos.
25.	Scissors	200mm	1 No.

C. TOOLS AND EQUIPMENT: (Computer Hardware - Installation and Maintenance)			
26.	Server Computer + with all accessories	Linux OS / VM Ware ESX(i)	01 Nos.
27.	Desktop Computer	CPU: 32/64 Bit i3/i5/i7 or latest processor, Speed: 3 GHz or Higher. RAM:- 16 GB DDR-IV or Higher, Wi-Fi Enabled. Network Card: Integrated Gigabit Ethernet, with USB Mouse, USB Keyboard and Monitor (Min. 17 Inch. Licensed Operating System and Antivirus compatible with trade related software. Or latest configuration	12 Nos.+ 01 Nos. (for Attacker server)
28.	Laptop, Notebook for demonstration		01 Nos.
29.	Printers: MFD		01 Nos.
30.	5KVA online UPS		As required
31.	LCD/DLP Projector/Interactive Smart Board		01No.
32.	Power Meter		02Nos.
33.	Computer Toolkits		06Nos.
D. SOFTWARE			
34.	Windows Server Operating System	Latest version	2 licenses
35.	Windows Operating System	Latest version	As required
36.	Linux Operating System	Latest version	As required
37.	Network Management Software	Latest version	As required
38.	MS Office	Latest version	As required
39.	Antivirus software	Latest version	As required
40.	Data recovery software	Latest version	As required
41.	APP SCAN		1 licence
CYBER SECURITY TOOLS			
42.	WIRESHARK	Latest version	As required
43.	Nmap	Latest version	As required
44.	Ncat (Netcat)	Latest version	As required
45.	Metasploit	Latest version	As required
46.	Nikto	Latest version	As required
47.	Burp Suite pro	Latest version	As required
48.	John the Ripper	Latest version	As required
49.	Aircrack-ng	Latest version	As required
50.	Nessus	Latest version	As required

51.	Snort	Latest version	As required
E. FURNITURE AND OTHER EQUIPMENTS			
52.	Computer Tables		12Nos.
53.	Computer Chairs		24Nos.
54.	Class room chairs		24 Nos.
55.	Air conditioners (optional)		As required
56.	Scanner		1 No.
57.	Modem		1 No.
58.	Broadband Internet connection		1 No.
59.	Firefighting equipment's	Arrange all proper NOCs and equipment's from Municipal/Competent authorities.	
F. COMPUTER NETWORKING			
60.	Wireless Access Point		6 Nos.
61.	L3 Router (Configurable)		1 No.
62.	Network Training System	This training system should help to understanding of Local Area Network (LAN) including fundamentals of networking. It should assist for knowledge of all network layers, cable designing and building of a complete network of computers. Students can study of various topologies using different standards given by IEEE with actual connections made in different topologies and data can be transferred. It should have provision to understand protocols, topologies used in networking, measurement of error rate, throughput and effect of errors on protocols. It should have PC to PC communication, Star topology, Ring topology.	2 Nos.
63.	LAN Protocol Simulation and Analyser Software (Trainer Kit)	Student can study Star, Bus & Ring selection, Protocols: CSMA /CD, CSMA /CA, Stop N Wait, Go back to N, Selective repeat, Sliding Window, Token Bus, Token Ring, Packet size: 128, 256, 512, 1024, 2048, 4096, 8192, 16384 Inter Packet delay: 1000 – 5000 ms.Indication of computer name, IP address, MAC address, Port number,	2 Nos.

		status of network, Network & protocol analysis like Indication of packet serial number.	
64.	Network and Internet security training kit	This training setup should help to students to understand Multimedia Computer and peripherals with artificial switch faults, to study the signals on various points 50MHz, 4 ch. Digital Storage Oscilloscope with more than 20 mpts memory should be available with this setup. Wireless Local Area Network, Managed Layer 2 and 3 Ethernet Switch 8 port--1 no each. Switch with POE ports-2 no.POE adapters-2no, Network Camera-1 no. Antivirus license Software for 1 year -2no. Fiber Optic cable with convertor, Media Converter - 2No. AC Supply: MCB with AC supply switches for safety purpose Horizontally aligned and sufficient legroom. It should provide with Power indicator & ON/OFF Control and Circuit Breaker of rating 3 Amp with ON/OFF Control and along with over load protection LAN Tester. Crimping Tool and RJ45 Connector with CAT6 cable.	2 Nos.
65.	RJ45 connectors		As required
66.	Multimeter	4 ½- digit large LCD displays with back light max. Reading: 1.9999, Voltage measurement up to 1000 VDC and 750V AC,DC, AC Current up to 20A,ACV frequency Response: 50KHz,Frequency, Resistance, Capacitance measurement, Diode check and Continuity test.	2Nos.

G. RAW MATERIAL			
67.	PCB, solder flux etc& electronic components		As required
68.	Wires, cables Plug sockets switches of various types and other consumables		As required
69.	Resistors, Capacitors, Inductors, Diodes, LED, Transistors, Thyristors, ICs etc.		As required
70.	Various types of Button Cells		As required
71.	Dry Cell		As required
72.	Hand Brush		As required
73.	Silicon grease		As required
74.	Heat sink agent		As required
75.	Cartridges for printer		As required
76.	3 Pin Power Chord		As required
77.	Flat Cable		100 meters
78.	Anti static pads		As required
79.	Anti static wrist wraps		As required
80.	Soldering wire and paste		As required
81.	RJ-11 connector		As required
82.	BNC connector, T connector, terminator		As required
83.	Keystone jack		As required
84.	LAN Card		As required
85.	Wi-Fi LAN Card both PCI and USB		As required

ANNEXURE-II

The DGT sincerely acknowledges contributions of the Industries, State Directorates, Trade Experts, Domain Experts, trainers of ITIs, NSTIs, faculties from universities and all others who contributed in revising the curriculum.

Special acknowledgement is extended by DGT to the following expert members who had contributed immensely in this curriculum.

List of Expert Members participated/ contributed for finalizing the course curriculum of Cyber Security Assistant trade held on 04.09.2023 at CSTARI, Kolkata			
S No.	**Name & Designation**	**Organization**	**Remarks**
1.	Mr. Sunil Kumar Gupta, DDG (ER)	CSTARI, Kolkata	Chairman
2.	Mr. N.R. Aravindan, Director	CSTARI, Kolkata	Member
3.	Mr. G.C. Saha, Joint Director	CSTARI, Kolkata	Member
4.	Mr. N.P. Bannibagi, Deputy Director	NIMI, Chennai	Member
5.	Mr. Abhishek Kumar, Deputy Director	STPI, Kolkata	Member
6.	Mr. MD Hussain Rabbani, Scientist “C”	ERTL (E), STQC, Kolkata	Member
7.	Mr. Sourav Sen, Advisory Technical Spec.	IBM, India	Member
8.	Mr. Asok Bandyopadhyay, Associate Director	C-DAC, Kolkata	Member
9.	Mr. Indrajit Bhattacharya, Principal Scientist	TCS, Kolkata	Member
10.	Mr. Niladri Roy, Consultant	TCS, Kolkata	Member
11.	Mr. Amit Kumar Mandal, Professor	Techno India University, Kolkata	Member
12.	Mr. Goutam Roy, Service Delivery Head	Prime Infoserve LLP, Kolkata	Member
13.	Mr. Amlan Raychaudhuri, Asst. Professor	BP Poddar Institute of Management & Technology, Kolkata	Member
14.	Mr. Prodip Mukhopadhyay, Sr. Advisor	MAKAUT, Kolkata	Member
15.	Mr. Avishek Paul, Asst. Professor	Techno India University, Kolkata	Member
16.	Mr. Arijit Sengupta, Asst.	TCS, Kolkata	Member

	Consultant		
17.	Mr. B. Sharanappa, Asst. Director	CSTARI, Kolkata	Member
18.	Mr. Bhagat Singh, Asst. Director	CSTARI, Kolkata	Member
19.	Mr. M.J. Vijay Raju, Asst. Director	CSTARI, Kolkata	Member
20.	Mr. Akhilesh Pandey, Asst. Director	CSTARI, Kolkata	Member
21.	Mr. B.K. Nigam, TO	CSTARI, Kolkata	Member
22.	Mr. K. V. S. Narayana, TO	CSTARI, Kolkata	Member
23.	Mr. P. K. Bairagi, TO	CSTARI, Kolkata	Member
24.	Mr. B. Biswas, TO	CSTARI, Kolkata	Member
25.	Mr. Anindya Sundar Das Gupta, Instructor	Women ITI, Banipur	Member
26.	Sarbojit Neogi, VI	NSTI, Kolkata	Member
27.	Mr. Jinendran PK, Junior Consultant	CSTARI, Kolkata	Member
28.	Mr. Sarvesh Singh, Junior Consultant	CSTARI, Kolkata	Member
29.	Mr. Sandeep, Junior Consultant	CSTARI, Kolkata	Member
30.	Mr. Pradip Biswas, Jr. D/man	CSTARI, Kolkata	Member

ABBREVIATIONS

CTS	Craftsmen Training Scheme
ATS	Apprenticeship Training Scheme
CITS	Craft Instructor Training Scheme
DGT	Directorate General of Training
MSDE	Ministry of Skill Development and Entrepreneurship
NTC	National Trade Certificate
NAC	National Apprenticeship Certificate
NCIC	National Craft Instructor Certificate
LD	Locomotor Disability
CP	Cerebral Palsy
MD	Multiple Disabilities
LV	Low Vision
HH	Hard of Hearing
ID	Intellectual Disabilities
LC	Leprosy Cured
SLD	Specific Learning Disabilities
DW	Dwarfism
MI	Mental Illness
AA	Acid Attack
PwD	Person with disabilities


कौशलं बलम्