



Competency Based Curriculum

CYBERSECURITY WITH AI

Diploma

མཁའ་འགྲུབ་
ཉམས་རིག



Technical Trainers Training and Resource Centre
Department of Workforce Planning and Skills Development
Ministry of Education and Skills Development

Published by Technical Trainers Training and Resource Center (TTTRC)
Department of Workforce Planning and Skills Development
Ministry of Education and Skills Development
Royal Government of Bhutan
Thimphu, Bhutan

Copyright © 2026 Technical Trainers Training and Resource Center (TTTRC)
Department of Workforce Planning and Skills Development

All rights reserved. No part of this book may be reproduced in any form without the permission from Technical Trainers Training and Resource Center, Department of Workforce Planning and Skills Development.

This book remains the property of the Department of Workforce Planning and Skills Development, MoESD.

First Edition: March, 2023

Second Edition June, 2026

ISBN 978-99980-792-4-3



དངལ་ལྷན་འབྲུག་གཞུང་། ཤེས་རིག་དང་རིག་ཆལ་གོང་འཕེལ་ལྷན་ཁག།
ལས་མི་འཆར་གཞི་དང་རིག་ཆལ་གོང་འཕེལ་ལས་ཁུངས།

Royal Government of Bhutan
Ministry of Education and Skills Development
Department of Workforce Planning and Skills
Development



Certificate No: *DWPSD/CEC-CS/2025-26/020*

Curriculum Endorsement Certificate

This is to certify that the curriculum for the following course(s) developed by

Technical Trainers Training and Resource Center

has been endorsed by the department.

Course	Level
Cybersecurity with AI	Diploma

Date of Endorsement: 30/06/2026



This certificate is valid till 29/06/2031 from the date of endorsement

Director General
Department of Workforce Planning and Skills Development

Foreword

Bhutan has seen a gradual increase in the requirement of skilled workers in recent years due to the growth of industries. However, the supply of skilled workforce that is responsive to the needs of the industry has not been able to keep pace with industry demand. Since skilled workers are a crucial ingredient for the socio-economic development of the country, it is important to have an adequate number of trained and certified workers. With growing industries, the “Cybersecurity Technologist” is not only a significant occupation but also in high demand in the labour market. In an effort to meet the skilled human resources requirement, it is imperative to deliver training based on the Competency Based Training system in Cybersecurity with AI Diploma to ensure a quality and adequate workforce in this sector.

To this end, the Department of Workforce Planning and Skills Development (DWPSD) is pleased to present the first edition of the Competency Based Curriculum for the Cybersecurity with AI Diploma course, developed with technical support from Humber Polytechnic, Canada and with funding from Global Affairs Canada (GAC) through the Bhutan Education and Skills Training (BEST) Project. Since it is an outcome of a more participatory process of curriculum development, it is expected to provide training delivery with reformed approaches, with its content being directly related to labour market needs, focusing on imparting skills and assessment based on industry work standards. We believe that the Competency Based Curriculum will help bridge the skill gap between industry needs and training institutes, thereby enhancing the employability of technical graduates.

The Department acknowledges the valuable contributions made by institutes and experts from relevant industries who were involved in the design and development of this curriculum. As it is a dynamic document that may require revision based on the needs of the changing labour market, the Department looks forward to receiving valuable feedback from institutes and industries to further improve and refine the curriculum. The Department hopes that this document will help advance Competency Based Learning in most of the TVET institutions.



(Phub Rinzin)

Director General

Department of Workforce Planning and Skills Development

Acknowledgement

Technical Trainers Training and Resource Center, Department of Workforce Planning and Skills Development would like to express our appreciation to the following subject experts and facilitators who have participated in the development and validation of curriculum for Cybersecurity Diploma:

Experts involved in the development of curriculum:

1. Mr. Tashi Wangchuk, Lecturer, Jigme Namgyel Engineering College (JNEC)
2. Mr. Younten Tshering, Lecturer, Jigme Namgyel Engineering College (JNEC)
3. Mr. Yeshe Jamtsho, Assoc. Lecturer, College of Science and Technology (CST)
4. Mr. Mohan Subba, ICT Officer, GovTech Agency
5. Ms. Pratima Pradhan, Deputy Chief ICT Officer, GovTech Agency
6. Ms. Passang Gyem, Network Administrator, Bhutan National Bank Ltd. (BNBL)
7. Mr. Pema Namgay, Freelancer, Thimphu

Experts involved in the validation of curriculum:

1. Mr. Yeshe Wangdi, Sr. Lecturer, Technical Training Institute-Rangjung, Trashigang
2. Mr. Jigme Lepcha, Chief Executive Officer, SAMU, Thimphu
3. Ms. Pratima Pradhan, Deputy Chief ICT Officer, GovTech Agency
4. Ms. Drishti Khampa, Associate IT engineer, Thimphu TechPark Ltd., Thimphu
5. Mr. Tenzin Dorji, Network Manager, NewEdge Technologies Pvt. Ltd, Thimphu
6. Mr. Ten Zing Dorjee, Associate Quality Assurance, Selise Bhutan, Thimphu
7. Mr. Chojay Wangchuk, Software Engineer, Selise Bhutan, Thimphu
8. Mr. Dawa Zangpo, ICT officer, World Wildlife Fund-Bhutan, Thimphu
9. Mr. Namkha Wangdi, System and Network Administrator, Royal Bhutan Police, Thimphu

Experts involved in the revision of curriculum:

1. Ms. Radikha Orari, Dy. Chief ICT Officer, GovTech Agency. Thimphu
2. Ms. Chanda man Limbu, ICT Officer, BNBL, Thimphu
3. Mr. Darshan Subedi, Network Engineer, BT, Thimphu
4. Mr. Jigme Nidup, Asst. Lecturer, TTI Rangjung
5. Mr. Sonam Tharchen, Asst. Lecturer, TTI Rangjung

Experts involved in the validation of curriculum:

1. Ms. Drishti Khampa, Lead CIE, Thimphu TechPark Ltd., Thimphu (**Chairperson**)
2. Mr. Ugyen Tshering, Manager, DC & Network, Bank of Bhutan
3. Ms. Menlam Choden, ICT Officer, GovTech Agency
4. Mr. Nima Wangchuk, Assistant ICT Officer, GovTech Agency
5. Mr. Sonam Tshering, Asst. Lecturer, TTI Rangjung
6. Mr. Sonam Tharchen, Asst. Lecturer, TTI Rangjung

Facilitators and editors for development and validation of curriculum:

1. Ms. Karma Dema, Program Officer, Technical Trainers Training and Resource Center (TTTRC)
2. Mr. Tshering Tobgay, Asst. Program Officer, Technical Trainers Training and Resource Center (TTTRC)

Chief editor

1. Mr. Karma Dorji, Offtg. Chief Program Officer, Technical Trainers Training and Resource Center (TTTRC)

Table of Contents

Foreword	1
Acknowledgement.....	2
Course Outline for Cybersecurity with AI, Diploma.....	4
Course Structure (2 Years Program).....	5
Course Information.....	9
Assessment and Certification System	10
Module Information:	12
Module 1.....	2
Managing network security.....	2
Apply network security controls.....	4
Perform network security need assessment.....	9
Manage and Monitor network security	13
Module 2.....	17
Managing system security	17
Manage system access and controls	19
Perform system hardening	23
Perform application and web security.....	27
Maintain information security	31
Module 3.....	35
Applying Artificial Intelligence in Cybersecurity Operations	35
Implement AI solutions for Cybersecurity.....	37
Analyze security data	41
Apply Adversarial AI Techniques.....	46
Annex I: Time Distribution Sheet.....	50
Annex II: Module Recognition	53
Annex IV: Lesson Plan.....	54
Annex V: Course Plan	60

Course Outline for Cybersecurity with AI, Diploma

Sl. No	Subject /Module	Duration (Hours)	Content Competencies (Mapped)
1.	Core modules	1596	CC
2.	OJT	420	CC
3.	Project work	140	
4.	Self-study	140	
5.	Summative and formative assessment	180	
Total		2476	
Generic Modules			
6.	Applied Dzongkha	42	SS
7.	Applied ICT	90	SS
8.	Applied Mathematics	126	SS
9.	Professional English Language	136	SS
10.	Ethics and integrity	68	PD
11.	Entrepreneurship	70	PD
12.	GNH and Human Values module	30	PD
Total		562	
Total Course Duration (Core Modules +OJT + Generic Modules)		2578	

Note: (*) This curriculum contains core modules which cover main competencies of Cybersecurity with AI Diploma and OJT components. There are separate curricula for subjects/modules for delivery of soft skills, professional development & values and environmental concern & safety. In order to achieve the qualification of Cybersecurity with AI Diploma, the subjects and modules listed must be accomplished as per the credit hours provided.

Content Competencies:

CC-Core Competencies

SS-Soft Skills

PD-Professional Development and Values

Course Structure (2 Years Program)

1. Semester 1

SL. No	Subject/Module	Duration (Hours)
1.	Module 1	497
2.	Applied mathematics-I	63
3.	Professional English -I	68
4.	GNH and Human Value	30
5.	Institute Assessment	35
Total Duration:		693

2. Semester 2

SL. No	Subject/Module	Duration (Hours)
1.	Module 2	518
2.	Applied mathematics-II	63
3.	Professional English -II	68
4.	Institute Assessment	35
Total Duration		684

3. Semester 3

SL. No	Subject/Module	Duration (Hours)
1.	Module 3	581
2.	Applied Dzongkha	42
3.	Institute Assessment	35
Total Duration:		658

4. Semester 4

SL. No	Subject/Module	Duration (Hours)
1.	OJT	420
2.	Ethics and Integrity	68
3.	Entrepreneurship	70
4.	Institute Assessment	35
5.	National Assessment	70
Total Duration:		663

Competency Profile

Trade: Cybersecurity with AI
Occupation: Cybersecurity Technologist

Competency Area	Sub- Competency Area	Competencies/Tasks 			
A: Manage network security	A1: Apply network security solutions	A1.01 Configure basic network devices	A1.02 Configure VLAN	A1.03 Configure VPN	A1.04 Configure firewall and IDS
	A2: Perform network security need assessment	A2.01 Maintain organization ICT asset inventory	A2.02 Determine threats and vulnerabilities	A2.03 Perform security assessment	A2.04 Analyze security assessment report
	A3: Manage and monitor network security	A3.01 Identify network security monitoring tools	A3.02 Deploy network security monitoring tools	A3.03 Analyze network security events	A3.04 Perform incident response
B: Manage system security	B1: Manage system access and controls	B1.01 Manage users	B1.02 Manage groups	B1.03 Manage file permissions	B1.04 Implement role-based access control
	B2: Perform system hardening	B2.01 Harden operating system	B2.02 Harden web server	B2.03 Harden database server	
	B3: Perform application and web security	B3.01 Perform vulnerabilities assessment	B3.02 Perform penetration testing	B3.03 Prepare recommendation report	
	B4: Maintain information security	B4.01 Classify information and data	B4.02 Maintain data confidentiality	B4.03 Maintain data integrity	B4.04 Perform data backup and recovery
C: Apply Artificial Intelligence in Cybersecurity Operations	C1: Implement AI solutions for Cybersecurity	C1.01 Identify cybersecurity tasks that can be optimized using AI tools	C1.02 Deploy AI solutions	C1.03 Apply AI solutions to solve cyber security tasks	C1.04 Verify AI solution performance against expected outcomes

	C2: Analyze Security Data	C2.01 Identify security data sources	C2.02 Deploy model locally	C2.03 Apply data analytics to identify patterns, indicators and anomalies	C2.04 Interpreting analysis results to support cybersecurity tasks
		C2.05 Predict potential security issues using analyzed data	C2.06 Validate effectiveness of security controls using analysis results		
	C3: Apply Adversarial AI Techniques	C3.01 Identify basic weaknesses in AI-based systems	C3.02 Apply simple adversarial techniques to test systems	C3.03 Conduct basic attack simulations on AI models	C3.04 Recommend improvements to strengthen AI system security

Course Information

COURSE TITLE	Cybersecurity with AI
LEVEL	Diploma
COURSE OBJECTIVE	Upon completion of Cybersecurity Diploma, the trainee will be able to: ● Manage network security; ● Manage system security; and ● Apply Artificial Intelligence in Cybersecurity Operations
COURSE DESCRIPTION	This course provides learners with the competencies to secure network and system infrastructures and apply Artificial Intelligence (AI) in modern cybersecurity operations. It focuses on identifying threats and vulnerabilities, implementing security controls, and managing access, system hardening, and incident response to protect organizational assets. Learners will also develop skills in analyzing security data and leveraging AI techniques to enhance threat detection, automate responses, and improve decision-making in dynamic cyber environments. The course emphasizes practical, hands-on skills aligned with current industry practices in cybersecurity and AI integration. To obtain the qualification of Cybersecurity Technologist, all learning outcomes prescribed for this qualification must be achieved.
TOTAL DURATION	Hours
TRAINING PROPORTION	1:12 (Practical) 1:20 (Theory)
ENTRY REQUIREMENT	● Completed Certificate 3 computer hardware and networking OR; ● Completed class 12 graduates
TRAINER QUALIFICATION	● Must have a minimum qualification of degree in a relevant field; ● Must have undergone Training of Trainers-Technical Instruction and Vocational Andragogy; ● Must have five years of work experience in a relevant field or internationally certified professional if the institute hires an industry expert as guest lecturer.

Assessment and Certification System

ASSESSMENT

Formative assessment for each module and learning outcome will be conducted using diverse methods such as assignments, project work, continuous assessment, practical demonstrations, observations, and oral or written assessments, with necessary reasonable accommodations and accessible assessment arrangements to ensure equitable opportunities for learners.

Summative assessment after completion of each national certificate level will be conducted by Bhutan Qualification and Professional Certificate Authority (BQPCA), MoESD as per the National Competency Standards and Guidelines for National Assessment and Certification System, provided the course is accredited with BQPCA, MoESD.

CERTIFICATION

On successful completion of course, the institute will award a certificate of achievement to the trainees. The Bhutan Qualification and Professional Certificate Authority (BQPCA), MoESD will award a National Certificate to the trainees upon the successful completion of each NC level assessment.

COURSE DELIVERY

1. Modular
2. Demonstration
3. Lecture
4. Universal Design of Learning (UDL)
5. Discussion with problem-based learning
6. Industrial training/attachment
7. Project work

RESOURCES

Materials

- Pen, pencil and paper

Software

Spreadsheet software, collaborative tools, Nmap, documentation tools, security assessment tools, firewall hardware, IDS tools (*e.g., PfSense, Snort, Suricata*), Wireshark/packet analyzer, firewall management console, IDS/IPS management tools, network diagnostic tools (*e.g., Ping, Traceroute*), network security monitoring tools, SIEM platform, technical note-taking tools (*e.g., Joplin, Obsidian*), virtualization software, Linux OS, operating systems, Windows Server, database software, visualization software, SSL Labs, Security Headers, vulnerability scanner, network scanning tools, exploitation tools (*e.g., Metasploit*), attack emulation tools (*e.g., Atomic Red Team*), backup tools (*e.g., Rsync*), encryption tools, web browser, AI security tools (*e.g., Wazuh MCP, SnortML, Burp Suite MCP*), performance monitoring and logging tools, benchmarking and evaluation framework tools, access to security tools and monitoring consoles, local model runtime (*e.g., Ollama, LM Studio, Jan*), open-weight AI models, Python with relevant libraries (*Matplotlib, Pandas*), data

analytics tools (*e.g., Power BI, Tableau, ELK*), Wazuh dashboard, OpenVAS, AI-integrated systems, diagramming tools, basic note-taking tools, AI testing interface or chatbot system, LLM playground or testing interface, test datasets or sample inputs, sandbox or cloned AI environment and adversarial tools (*e.g., ART, CleverHans*).

Equipment

- Computer with internet connectivity, router, switch, Access point, cable (fiber/ethernet), SFP, VM with Ubuntu OS, network devices, virtual machine/server, workstation with sufficient RAM/VRAM and disk space with internet connectivity (*for initial model download*)

PPE

- Working dress and safety boot

Learning Materials

- Competency Based Learning Materials (CBLM)
- Reference books
- Hand-outs
- Audio visuals

Infrastructure and training facilities

- **Theory classroom size:** Minimum of 1 m² per trainee;
- **Practical Workshop size:** Minimum of 2.25 m² per trainee. Variables must be considered depending upon the type of skills being taught and the number of trainees participating at a time.

Module Information:
Cybersecurity with AI

Module 1

Managing network security

MODULE INFORMATION

Occupation	Cybersecurity Technologist
Competency Area	Manage network security
Module Title	Managing network security
Module Code	2529-L4-M1
Module Description	This module is structured to provide learners with the knowledge, skills and right attitude required to perform organizational security -assessment, apply network security controls, monitor network security and manage security information and events.
Nominal Duration	497 Hours
Certificate Level	Diploma
Pre-requisite	• Completed NC3 computer hardware and networking or; • Completed class 12 graduates.
Learning Outcome	1. Apply network security solutions 2. Perform network security need assessment 3. Manage and monitor network security

Module Title	Managing network security		
Module Code	2529-L4-M1		
Learning Outcome 1	Apply network security controls		
Duration	Theory: 70 hours	Practical: 70 hours	Total: 140 hours
Assessment Criteria	- Basic Network device is configured as per the job requirement following standard procedure - VLAN is configured as per the job requirement following standard procedure - VPN is configured as per the job requirement following standard procedure - Firewall and IDS is configured as per the job requirement following standard procedure - Network security issues are troubleshot as per the job requirement following standard procedure		
Content	A1.00 Introductory knowledge - Introduction to cybersecurity module - Importance of cybersecurity - Roles of cybersecurity technologist - Introduction to CIA (Confidentiality, Integrity, Availability) triads - Scopes and trends of cybersecurity technologist - Awareness on Intellectual Property Right (IPR) - Ethical principle for cybersecurity professionals - Introduction to National Cybersecurity Legislation, Policy and Strategies - Domains of cybersecurity - Introduction to basic programming A1.01 Configuring basic Network devices Knowledge - Introduction to network and OSI model - Introduction to network architecture - Introduction to IP addressing, subnetting and CIDR notation - Introduction to CLI commands and its function - Function and types of routers, switches and Access points (AP) - Types of network protocols such as TCP/IP, UDP and ICMP - Network zones (DMZ, Internal, User) - Categories of ports and common services - Basic networking commands Skills - Network topology designing skills - Switching and routing skills - Diagnostic skills - ICT skills - Communication skills - Observation skills		

	• Analytical skills • Planning skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Effective time management • Responsible configuration of network systems to prevent unauthorized access • Attention to network reliability and security impact of configurations • Encouraging inclusive participations • Being vigilant and patient • Ethical handling organizational network infrastructure • Proper handling of tools, materials and equipment • Having sense of ownership and accountability • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation A1.02 Configuring VLAN <i>Knowledge</i> • Introduction to VLAN • Segregation of VLAN and its purpose • Introduction to VLAN mapping • Functions of commands used in creating VLAN <i>Skills</i> • Routing and switching skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Numeracy skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Being aware of network segmentation for security protection • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Being vigilant and patient while configuring • Having work ethics and integrity • Proper handling of tools, materials and equipment • Having sense of ownership and accountability • Ensuring appropriate use of PPE • Ensuring proper disposal of waste
--	--

	• Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation A1.03 Configuring VPN Knowledge • Introduction to VPN technologies • Types of VPN (Remote Access, Site-to-Site) • VPN protocols (IPsec, SSL/TLS, L2TP, PPTP) • Encryption and authentication methods Skills • VPN Configuration skill • Network topology designing skills • Switching and routing skills • ICT skills • Observation skills • Communication skills • Analytical skills • Planning skills • Problem solving skill Attitude, safety and environmental concern • Having respect for confidentiality and secure communication • Ethical responsibility when handling encrypted connections and user data • Being aware of privacy protection in remote access systems • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Having work ethics and integrity • Proper handling of tools, materials and equipment • Having sense of ownership and accountability • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation A2.04 Configuring Firewall and IDS Knowledge • Definition and purpose of firewalls and Intrusion Detection Systems (<i>IDS</i>) • Types of firewalls and Intrusion Detection Systems (<i>IDS</i>) • Common IDS tools and its uses • Difference between IDS and IPS (<i>Intrusion Prevention System</i>) • Access Control Lists (<i>ACLs</i>) • Categories of ports and common services • Methods of detection (<i>signature based and anomaly-based detection</i>) • Concept of false positive and false negative
--	---

	Skills • Basic network management skills • Firewall & IDS configuration skills • Analytical skills • Basic Linux/ CLI (Command-Line Interface) skills • ICT skills • Communication skills • Observation skills • Planning skills • Problem solving skill Attitude, safety and environmental concern • Ethical responsibility in configuring security controls • Being accountable in monitoring and responding to threats • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Being vigilant in identifying false positives/false negatives impacts • Having work ethics and integrity • Proper handling of tools, materials and equipment • Having sense of ownership and accountability • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation
Learning Conditions	Learning Materials • Competency Based Learning Materials (CBLM)/Reference materials • Hand-outs • Audio Visuals • Reference books • Manuals Learning Facilities and infrastructure • Classroom with adequate facilities • Information Technology (IT) lab • Library Materials • Pen, pencil and paper Software • Firewall/hardware, IDS tools (<i>Eg. Pfsense, snort, suricata, etc</i>), packet tracer, firewall management console, IDS/IPS management tools and network diagnostic tools (<i>Eg. Ping, traceroute, Nmap</i>)

	Equipment - Router, switch, Access point, cable (fiber/ethernet), SFP, VM with Ubuntu OS, network devices and Computer with internet connectivity PPE - Working dress and safety boot
Instructional Methodologies	The trainer shall use <i>inter alia</i>, the following instructional methods: - Lecture - Interactive discussion - Demonstration - Industrial visit/training - Guided practice - Group practice with project-based learning - Individual practice with problem-based learning - Universal Design of Learning (UDL)
Method of Assessment	The trainer shall use <i>inter alia</i>, the following assessment methods: - Practical observation - Oral/viva-voce - Written test - Assignment - Project work

Module Title	Managing network security		
Module Code	2529-L4-M1		
Learning Outcome 2	Perform network security need assessment		
Duration	Theory: 35 hours	Practical: 119 hours	Total: 154 hours
Assessment Criteria	- Organizations ICT assets inventory is developed as per the job requirement following standard procedure - Threats and vulnerabilities are determined as per the job requirement following standard procedure - Security assessment is performed as per the job requirement following standard procedure - Security assessment report is analyzed as per the job requirement following standard procedure		
Content	A2.01 Maintaining organization ICT asset inventory Knowledge - Functions of different network devices - Definition of assets - Categories of ICT assets - Importance of record keeping - Document versioning Skills - Record management skills - ICT skills - Communication skills - Observation skills - Analytical skills - Planning skills - Problem solving skill Attitude, safety and environmental concern - Ethical handling of organizational data and ICT assets - Confidentiality and responsibility in managing ICT inventory - Effective time management - Being efficient in using resources - Encouraging inclusive participations - Being vigilant and patient - Ensuring appropriate use of PPE - Ensuring proper disposal of waste - Ensuring to follow environmental rules and regulations - Ensuring to follow OHS rules and regulation - Ensuring to keep backup copies or store inventory book in the safe location A2.02 Determining threats and vulnerabilities Knowledge - Definition of security		

	• Types of security ✓ Network security ✓ Cloud security ✓ Information security ✓ Physical security • Importance of network security • Definition of threat, vulnerability and risk • Types of threats • Process of risk management • Introduction to NIST cyber security risk management framework • Threat intelligence fundamentals Skills • Networking skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Problem solving skill Attitude, safety and environmental concern • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Being vigilant against misuse of security findings • Having ethical responsibility in reporting vulnerabilities • Proper handling of tools, materials and equipment • Having sense of ownership and accountability • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation A2.03 Performing security need assessment Knowledge • Network security concepts and principles • Vulnerability Assessment and Penetration Testing (VAPT) concepts and methodologies • Wireless network security standards • Threat intelligence Tools Skills • Documentation skills • ICT skills • Communication skills
--	---

	• Observation skills • Analytical skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Being vigilant and accountable in security decision-making • Having integrity in security assessment reporting • Ethical handling of vulnerabilities and sensitive findings • Proper handling of tools, materials and equipment • Having sense of ownership and accountability • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow OHS rules and regulation A2.04 Analyzing security assessment report <i>Knowledge</i> • Security assessment methodologies • Risk management frameworks (<i>ISO 27001, NIST</i>) • Vulnerability classification (<i>CVSS scoring</i>) • Compliance and regulatory requirements <i>Skills</i> • Analytical skills • ICT skills • Communication skills • Observation skills • Planning skills <i>Attitude, safety and environmental concern</i> • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Being vigilant and patient • Ethical interpretation of security findings (avoid bias or misuse) • Being a team player • Having responsibility and accountability • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation
Learning Conditions	Learning Materials • Competency Based Learning Materials (CBLM)/Reference materials • Hand-outs

	• Audio Visuals • Reference books • Manuals Learning Facilities and infrastructure • Classroom with adequate facilities • Information Technology (IT) lab • Library Materials • Pen, pencil and paper Software • Spreadsheet software, collaborative tools, Nmap, documentation tools and security assessment tools Equipment • Computer with internet connectivity, router, switches and access points PPE • Working dress and safety boot
Instructional Methodologies	The trainer shall use <i>inter alia</i>, the following instructional methods: • Lecture • Interactive discussion • Demonstration • Industrial visit/training • Guided practice • Group practice with project-based learning • Individual practice with problem-based learning • Universal Design of Learning (UDL)
Method of Assessment	The trainer shall use <i>inter alia</i>, the following assessment methods: • Practical observation • Oral/viva-voce • Written test • Assignment • Project work

Module Title	Managing network security		
Module Code	2529-L4-M1		
Learning Outcome 3	Manage and Monitor network security		
Duration	Theory: 56 hours	Practical: 147 hours	Total: 203 hours
Assessment Criteria	• Network security monitoring tools are identified as per the job requirement following standard procedure • Network security monitoring tools are deployed as per the job requirement following standard procedure • Network security events are analyzed as per the job requirement following standard procedure • Incident response is performed as per the job requirement following standard procedure		
Content	A3.01 Identifying network security monitoring tools Knowledge • Types of network security monitoring tools • Introduction to Security Information and Event Management (SIEM) • SIEM platforms (Splunk, QRadar, Wazuh) • Netflow and traffic analysis • Open-source vs commercial tool evaluation • Network traffic analysis techniques • Packet capture (Wireshark, tcpdump) • Common network attacks and indicators Skills • Research and information gathering skills • Analytical and evaluation skills • ICT skills • Communication skills • Observation skills • Planning skills • Problem solving skills • Report writing skills Attitude, safety and environmental concern • Being responsible while evaluating security technologies • Effective time management • Being efficient in using resources • Being vigilant and patient • Having ethics and integrity while reporting tool capabilities • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation		

	A3.02 Deploying network security monitoring tools Knowledge • Definition of network traffic, bandwidth, latency, packet loss and round-trip time (RTT) • Network security monitoring protocols such as SNMP, NetFlow, Remote Monitoring (RMON), etc. Skills • Basic network management skills • Linux commands • Diagnostic skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Problem solving skill Attitude, safety and environmental concern • Being responsible in ensuring continuous monitoring accuracy • Being aware about impact of missed alerts or misconfigured monitoring • Ethical handling of network security monitoring tools • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation A3.03 Analyzing network security events Knowledge • Introduction to cybersecurity incident Triage • Security event and log analysis • MITRE ATT&CK framework • Threat intelligence and IOCs • Incident classification and severity levels Skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Problem solving skill
--	---

	<i>Attitude, safety and environmental concern</i> • Being responsible and accurate while classifying incidents • Effective time management • Being efficient in using resources • Being vigilant and patient • Encouraging inclusive participations • Having work ethics and integrity • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation A3.04 Performing incident response <i>Knowledge</i> • Introduction to cybersecurity Incident Response • Introduction to Sandbox, isolations of infected devices • Process of disaster Recovery • Process of business continuity • Incident response procedures <i>Skills</i> • OS/network skills • Documentation skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Being calm and vigilant during cyber incident • Being accountable in containment and recovery actions • Ethical responsibility in incident handling and reporting • Having integrity during forensic and recovery processes • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Being a team player • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation
Learning Conditions	Learning Materials • Competency Based Learning Materials (CBLM)

	• Hand-outs • Audio Visuals • Reference books • Manuals Learning Facilities and infrastructure • Classroom with adequate facilities • Information Technology (IT) lab • Library Materials • Pen, pencil and paper Software • Network security monitoring tools, SIEM platform, IPS/IDS management console and documentation tools (<i>technical note taking tools-eg joplin,obsidian</i>) Equipment • Computer with internet connectivity and server PPE • Working dress and safety boot
Instructional Methodologies	The trainer shall use <i>inter alia</i>, the following instructional methods: • Lecture • Interactive discussion • Demonstration • Industrial visit/training • Guided practice • Group practice with project-based learning • Individual practice with problem-based learning • Universal Design of Learning (UDL)
Method of Assessment	The trainer shall use <i>inter alia</i>, the following assessment methods: • Practical observation • Oral/viva-voce • Written test • Assignment • Project work

Module 2

Managing system security

MODULE INFORMATION

Occupation	Cybersecurity Technologist
Competency Area	Manage system security
Module Title	Managing system security
Module Code	2529-L4-M2
Module Description	This module is structured to provide learners the knowledge, skills and right attitude required to perform system hardening, managing system access & controls, assess application security and apply information security.
Nominal Duration	518 Hours
Certificate Level	Diploma
Pre-requisite	Completed 2529-L4-M1
Learning Outcome	1. Perform system hardening 2. Perform system access and controls 3. Assess application security 4. Apply information security

Module Title	Managing system security		
Module Code	2529-L4-M2		
Learning Outcome 1	Manage system access and controls		
Duration	Theory: 20 hours	Practical: 29 hours	Total: 49 hours
Assessment Criteria	• Users are managed as per the job requirement following standard procedure • Groups are managed as per the job requirement following standard procedure • File permission are managed as per the job requirement following standard procedure • Role based access control are implemented as per the job requirement following standard procedure		
Content	B1.01 Managing users Knowledge • Introduction to Operating System • Definition of users • Types of users • Text-based database of user (<i>passwd and shadow file</i>) • Basic Linux Commands (<i>Create, Modify, delete, etc</i>) Skills • System Administration skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Numeracy skills • Problem solving skill Attitude, safety and environmental concern • Having respect for confidentiality of user credentials and system data • Ethical responsibility in user account management • Being accountable in granting and revoking access rights • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation B1.02 Managing groups Knowledge • Definition of group • Commands to manage groups • Text-based group information database (<i>group and gshadow file</i>)		

	<i>Skills</i> • System Administration skills • Using Linux commands • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Numeracy skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Being responsible in grouping users correctly to avoid unauthorized access • Being aware about role-based access control principle • Having integrity while managing user roles and privileges • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation B1.03 Managing file permission <i>Knowledge</i> • Basic Linux Command (<i>Create files, directory, copy, move, etc</i>) • File system structure (<i>hierarchy</i>) • Level of file permissions (<i>read, write, and execute</i>) • Method of permission assignment (<i>absolute and symbolic</i>) • Commands to manage file permissions (<i>ls, chmod, chown, chgrp, umask</i>) <i>Skills</i> • System Administration skills • Using Linux commands • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Numeracy skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Being aware about security risk from incorrect file permission • Being responsible in protecting sensitive system files • Being attentive to least privilege principle in permission assignment
--	--

	• Ethical handling of system configuration changes • Effective time management • Encouraging inclusive participations • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation B1.04 Implementing role-based access controls <i>Knowledge</i> • Introduction to access control • Types of access control • Introduction to Active Directory Architecture • Introduction to User and group management • Introduction to Computer management • Group Policy (<i>security settings and permissions across the domain</i>) <i>Skills</i> • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Being accountable in assigning roles and permissions • Ethical responsibility in enforcing access control policies • Being aware of security impact of RBAC misconfiguration • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Being vigilant and patient • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation
Learning Conditions	Learning Materials • Competency Based Learning Materials (CBLM) • Hand-outs • Audio Visuals • Reference books • Manuals

	Learning Facilities and infrastructure • Classroom with adequate facilities • Information Technology (IT) lab • Library Materials • Pen, pencil and paper Software • Virtualization software, operating systems (<i>windows and Linux</i>) Equipment • Computer with internet connectivity and server PPE • Working dress and safety boot
Instructional Methodologies	The trainer shall use <i>inter alia</i>, the following instructional methods: • Lecture • Interactive discussion • Demonstration • Industrial visit/training • Guided practice • Group practice with project-based learning • Individual practice with problem-based learning • Universal Design of Learning (UDL)
Method of Assessment	The trainer shall use <i>inter alia</i>, the following assessment methods: • Practical observation • Oral/viva-voce • Written test • Assignment • Project work

Module Title	Managing system security		
Module Code	2529-L4-M2		
Learning Outcome 2	Perform system hardening		
Duration	Theory: 49 hours	Practical: 70 hours	Total: 119 hours
Assessment Criteria	- Operating system is hardened as per the job requirement following standard procedure - Web server is hardened as per the job requirement following standard procedure - Data base server is hardened as per the job requirement following standard procedure		
Content	B2.01 Hardening operating systems Knowledge - Introduction to system security and system hardening - Types of Operating Systems - Disk partitions and encryptions - RAID configuration - Introduction to BIOS and UEFI - Introduction to physical access controls - IP addresses configuration - User account management - Account password Policies - Best practices for Operating System hardening (<i>CIS benchmark and equivalent</i>) Skills - Network management skills - Linux command - ICT skills - Communication skills - Observation skills - Analytical skills - Planning skills - Problem solving skill Attitude, safety and environmental concern - Being responsible in securing system configurations against threats - Being aware of consequences of misconfiguration on system security - Ethical handling of privileged system access - Effective time management - Being efficient in using resources - Encouraging inclusive participation - Ensuring appropriate use of PPE - Ensuring proper disposal of waste - Ensuring to follow environmental rules and regulations		

	- Ensuring to follow OHS rules and regulation B2.02 Hardening web server Knowledge - Introduction to DNS - Types of Web servers - Application deployment architecture - Web server configuration - Introduction to Web protocols (<i>HTTP, HTTPS and TLS/SSL</i>) - Request/Response Headers and status codes - Access and error log formats - Best practices for hardening web server (<i>CIS benchmark and equivalent</i>) Skills - Network management skills - Basic Linux Commands - Server Administration skills - ICT skills - Communication skills - Observation skills - Analytical skills - Planning skills - Numeracy skills - Problem solving skill Attitude, safety and environmental concern - Being responsible in securing web services handling public data - Being aware of impact of insecure web configurations (data breaches, attacks) - Ethical responsibility in managing web server logs and access data - Attention to secure communication standards (HTTPS/TLS) - Effective time management - Being efficient in using resources - Encouraging inclusive participations - Ensuring appropriate use of PPE - Ensuring proper disposal of waste - Ensuring to follow environmental rules and regulations - Ensuring to follow OHS rules and regulation B2.03 Hardening database server Knowledge - Introduction to database management system - Types of database - Introduction to Data encryption - Database configurations - Types of database users
--	--

	• Concept of database language • Database audit log • Concept of database import and export (<i>backup and restore</i>) • Best practices of hardening database server (<i>CIS benchmark and equivalent</i>) Skills • Network management skills • Database management skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Numeracy skills • Problem solving skill Attitude, safety and environmental concern • Being responsible in protecting sensitive data integrity and confidentiality • Ethical handling of database access and credentials • Being aware of risks of data leakage and unauthorized access • Being accountable in in backup and recovery processes • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation
Learning Conditions	Learning Materials • Competency Based Learning Materials (CBLM) • Hand-outs • Audio Visuals • Reference books • Manuals Learning Facilities and infrastructure • Classroom with adequate facilities • Information Technology (IT) lab • Library • Workshop Materials • Pen, pencil and paper Software • Operating system, database software, visualization software and SSL labs

	Equipment • Computer with internet connectivity and server PPE • Working dress and safety boot
Instructional Methodologies	The trainer shall use <i>inter alia</i>, the following instructional methods: • Lecture • Interactive discussion • Demonstration • Industrial visit/training • Guided practice • Group practice with project-based learning • Individual practice with problem-based learning • Universal Design of Learning (UDL)
Method of Assessment	The trainer shall use <i>inter alia</i>, the following assessment methods: • Practical observation • Oral/viva-voce • Written test • Assignment • Project work

Module Title	Managing system security		
Module Code	2529-L4-M2		
Learning Outcome 3	Perform application and web security		
Duration	Theory: 61 hours	Practical: 170 hours	Total: 231 hours
Assessment Criteria	• Vulnerabilities assessment is performed as per the job requirement following standard procedure • Penetration testing is performed as per the job requirement following standard procedure • Recommendation report is prepared as per the job requirement following standard procedure		
Content	B3.01 Performing vulnerability assessment <i>Knowledge</i> • Introduction to ethical hacking • Different application related threats • Introduction to OWASP Top 10 • Types of vulnerabilities • Vulnerabilities related to API and Library • Common Vulnerability Scoring System (CVSS) • Awareness on cyber related laws and regulations <i>Skills</i> • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Numeracy skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Ethical responsibility in vulnerability discovery and disclosure • Having integrity in handling security findings (no misuse of exploits) • Being responsible in reporting risks accurately • Being aware about system boundaries and authorization rules • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation B3.02 Performing penetration testing <i>Knowledge</i> • Concept of Penetration Testing Execution Standards (PTES) • Process of PTES		

	• Introduction to Attack tactics • Purpose of penetration testing • Types of penetration testing • Process of penetration testing • Techniques of penetration testing • Introduction to Common Vulnerability and Exposure (CVE) databases • Introduction to Exploit-DB Skills • Scripting skills • Using Linux command • System administration skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Numeracy skills • Problem solving skill Attitude, safety and environmental concern • Adhering to authorization and legal boundaries in testing • Ethical responsibility during exploitation activities • Having integrity in documenting findings without exaggeration • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation B3.03 Preparing recommendation report Knowledge • Report writing format/template • Types of VAPT reports (<i>Executive summary, Technical Vulnerability Assessment, Penetration Testing, Compliance, Remediation</i>) Skills • Presentation skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Numeracy skills • Problem solving skill
--	--

	<i>Attitude, safety and environmental concern</i> • Having ethics and integrity while handling sensitive security findings • Being accountable in providing recommendations for remediation • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Being vigilant and patient • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulations
Learning Conditions	Learning Materials • Competency Based Learning Materials (CBLM) • Hand-outs • Audio Visuals • Reference books • Manuals Learning Facilities and infrastructure • Classroom with adequate facilities • Information Technology (IT) lab • Library • Workshop Materials • Pen, pencil and paper Software • Vulnerability scanner, network scanning tools, virtualization tools, exploitation tools (<i>eg: Metasploit</i>), burp suite, attack emulation tools (<i>Eg. Atomic red team</i>) and documentation tools Equipment • Computer with internet connectivity and server PPE • Workshop dress and safety boot
Instructional Methodologies	The trainer shall use <i>inter alia</i>, the following instructional methods: • Lecture • Interactive discussion • Demonstration • Industrial visit/training • Guided practice • Group practice with project-based learning • Individual practice with problem-based learning • Universal Design of Learning (UDL)

Method of Assessment	The trainer shall use <i>inter alia</i>, the following assessment methods: • Practical observation • Oral/viva-voce • Written test • Assignment • Project work
-----------------------------	---

Module Title	Managing system security		
Module Code	2529-L4-M2		
Learning Outcome 4	Maintain information security		
Duration	Theory: 28 hours	Practical: 91 hours	Total: 119 hours
Assessment Criteria	- Information and data are classified as per the job requirement following standard procedure - Data confidentiality is maintained as per the job requirement following standard procedure - Data integrity is maintained as per the job requirement following standard procedure - Data backup and recovery is performed as per the job requirement following standard procedure		
Content	B4.01 Classifying information and data <i>Knowledge</i> - Definition of information and data - Purpose of data classification - Categories of data classification - Introduction to data governance framework of Bhutan - Introduction to data protection laws - Importance of information and data security <i>Skills</i> - ICT skills - Communication skills - Observation skills - Analytical skills - Planning skills - Numeracy skills - Problem solving skill <i>Attitude, safety and environmental concern</i> - Proper handling of classified/sensitive information - Ethical awareness in data access and sharing - Being accountable in maintaining data governance compliance - Effective time management - Being efficient in using resources - Encouraging inclusive participations - Ensuring appropriate use of PPE - Ensuring proper disposal of waste - Ensuring to follow environmental rules and regulations - Ensuring to follow OHS rules and regulation B4.02 Maintaining data confidentiality - Introduction to cryptography - Introduction to CIA Triad - Definition of data confidentiality and privacy		

	• Importance of data confidentiality • Introduction to symmetric and asymmetric ciphers <i>Skills</i> • Basic Linux command • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Numeracy skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Having respect for privacy and sensitive information • Having ethical responsibility in handling encrypted and private data • Being aware about consequences of data breaches • Having integrity in managing confidential systems and credentials • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation B4.03 Maintaining data integrity <i>Knowledge</i> • Definition of data integrity • Application of data integrity • Importance of maintaining data integrity • Different hashing algorithms • Advantages of hashing algorithms • Introduction to AES and RSA algorithms • Data Loss Prevention <i>Skills</i> • Basic Linux command • ICT skills • Communication skills • Observation skills • Analytical skills • Numeracy skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Ethical responsibility in preventing unauthorized data changes • Attention to detail in validating system outputs
--	---

	• Being accountable in maintaining secure data systems • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Being vigilant and patient • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation B4.04 Performing data backup and recovery <i>Knowledge</i> • Definition of data availability • Importance of data backup and recovery • Techniques of data backup • Concept on manual and automated backup • Introduction to backup storage options • Process of disaster recovery planning <i>Skills</i> • Documentation skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Numeracy skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Being responsible in ensuring data availability and recovery readiness • Being aware of impact of data loss on operations and services • Being accountable in disaster recovery planning and execution • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation
Learning Conditions	Learning Materials • Competency Based Learning Materials (CBLM) • Hand-outs • Audio Visuals • Reference books • Manuals

	Learning Facilities and infrastructure • Classroom with adequate facilities • Information Technology (IT) lab • Library Materials • Pen, pencil and paper Software • Spreadsheet software, backup tools, rsync and encryption tools Equipment • Computer with internet connectivity, router, access point, switch and server PPE • Working dress and safety boot
Instructional Methodologies	The trainer shall use <i>inter alia</i>, the following instructional methods: • Lecture • Interactive discussion • Demonstration • Industrial visit/training • Guided practice • Group practice with project-based learning • Individual practice with problem-based learning • Universal Design of Learning (UDL)
Method of Assessment	The trainer shall use <i>inter alia</i>, the following assessment methods: • Practical observation • Oral/viva-voce • Written test • Assignment • Project work

Module 3

Applying Artificial Intelligence in Cybersecurity Operations

MODULE INFORMATION

Occupation	Cybersecurity Technologist
Competency Area	Apply Artificial Intelligence in Cybersecurity Operations
Module Title	Applying Artificial Intelligence in Cybersecurity Operations
Module Code	2529-L4-M3
Module Description	This module is structured to provide learners the knowledge, skills and right attitude required to implement AI solutions for cyber security, analyze security data and apply adversarial AI Techniques
Nominal Duration	581 Hours
Certificate Level	Diploma
Pre-requisite	Completed 2529-L4-M2
Learning Outcome	1. Implement AI solutions for Cybersecurity 2. Analyze Security Data 3. Apply Adversarial AI Techniques

Module Title	Apply Artificial Intelligence in Cybersecurity Operations		
Module Code	2529-L4-M3		
Learning Outcome 1	Implement AI solutions for Cybersecurity		
Duration	Theory: 49 hours	Practical: 84 hours	Total: 133 hours
Assessment Criteria	• Cybersecurity tasks that can be optimized using appropriate AI tools are identified as per the job requirement following standard procedure • AI solutions are deployed as per the job requirement following standard procedure • AI solutions are applied as per the job requirement following standard procedure • AI solutions are verified against expected outcomes as per the job requirement following standard procedure		
Content	C1.01 Identifying cybersecurity tasks that can be optimized using AI tools Knowledge • Introduction to AI • Introduction to AI enhanced attacks • Introduction to AI tools for cybersecurity • Basic cybersecurity tasks (<i>monitoring, detection, logging</i>) • Common AI tools used in cybersecurity (<i>Eg. Wazuh MCP, SnortML</i>) • Usage of AI in cybersecurity • Workflow automation tools (<i>Eg. n8n, Zapier</i>) Skills • Research skills • ICT skills • Communication skills • Analytical skills • Planning skills • Report writing skills Attitude, safety and environmental concern • Ethical awareness in AI-assisted cybersecurity decisions • Being responsible in identifying risks of AI misuse (AI-enhanced attacks) • Being accountable in selecting appropriate AI tools for security tasks • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation C1.02 Deploying AI solutions Knowledge • Introduction to MCP and agentic AI • Introduction to tools like WazuhMCP, burp suite MCP and SnortML • AI solution deployment lifecycle		

	<i>Skills</i> • Cybersecurity skills • ICT and installation skills • Communication skills • Observation skills • Analytical skills • Planning skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Being responsible in secure deployment of AI systems • Being aware of risks of autonomous AI actions • Ethical use of agentic AI systems in cybersecurity environments • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Being vigilant and patient • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation C1.03 Applying AI solutions to solve cyber security tasks <i>Knowledge</i> • AI tool's dashboard or interfaces • Importance of AI model training • Introduction to prompt engineering • Incident Response Automation • Introductions baseline setting <i>Skills</i> • Cybersecurity skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Being responsible in interpretation of AI-generated security alerts • Being aware of false positives/negatives in AI systems • Having integrity in validating AI-assisted decisions • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Being vigilant and patient
--	--

	• Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation C1.04 Verifying AI solutions against expected outcomes Knowledge • AI model evaluation metrics (<i>confusion matrix, accuracy, precision, recall, F1 score</i>) • Performance benchmarking techniques • Introduction to policy tuning and improvement (<i>Example: improving existing security device configuration</i>) Skills • Cybersecurity skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Problem solving skill Attitude, safety and environmental concern • Being responsible in ensuring AI model reliability before deployment • Being accountable for incorrect AI-driven security decisions • Ethical responsibility in avoiding over-reliance on AI outputs • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation
Learning Conditions	Learning Materials • Competency Based Learning Materials (CBLM) • Hand-outs • Audio Visuals • Reference books • Manuals Learning Facilities and infrastructure • Classroom with adequate facilities • Information Technology (IT) lab • Library

	Materials • Pen, pencil and paper Software • Web browser, AI security tools (<i>Eg. Wazuh MCP, SnortML, Burp suite MCP</i>), Documentation tools, performance monitoring and logging tools and benchmarking & evaluation framework tools Equipment • Computer with internet connectivity and virtual machine/server PPE • Working dress and safety boot
Instructional Methodologies	The trainer shall use <i>inter alia</i>, the following instructional methods: • Lecture • Interactive discussion • Demonstration • Industrial visit/training • Guided practice • Group practice with project-based learning • Individual practice with problem-based learning • Universal Design of Learning (UDL)
Method of Assessment	The trainer shall use <i>inter alia</i>, the following assessment methods: • Practical observation • Oral/viva-voce • Written test • Assignment • Project work

Module Title	Apply Artificial Intelligence in Cybersecurity Operations		
Module Code	2529-L4-M3		
Learning Outcome 2	Analyze security data		
Duration	Theory: 119 hours	Practical: 168 hours	Total: 287 hours
Assessment Criteria	- Relevant cybersecurity data sources are identified as per the job requirement following standard procedure - Models are deployed locally as per the job requirement following standard procedure - Patterns, indicators and anomalies are identified by applying data analytics as per the job requirement following standard procedure - Analysis result is interpreted as per the job requirement following standard procedure - Potential security issues are predicted as per the job requirement following standard procedure - Effectiveness of security controls are validated as per the job requirement following standard procedure		
Content	C2.01 Identifying security data sources Knowledge - Types of security data sources (<i>logs, events, alerts, flow data, packet captures</i>) - Log formats and transport protocols (<i>syslog, JSON, CSV, NetFlow, SNMP</i>) - Introduction to SIEM data model and event taxonomy - Introduction to data source cataloging Skills - Research and information gathering skills - Documentation skills - ICT skills - Communication skills - Analytical skills - Planning skills - Report writing skills Attitude, safety and environmental concern - Being responsible in handling sensitive log and security data - Being aware of data privacy when accessing logs - Ethical use of monitoring data - Effective time management - Being efficient in using resources - Encouraging inclusive participations - Ensuring appropriate use of PPE - Ensuring proper disposal of waste - Ensuring to follow environmental rules and regulations - Ensuring to follow OHS rules and regulation		

	C2.02 Deploying AI model locally Knowledge • Introduction to Large Language Models (LLMs) and open-weight vs proprietary models • Concept of local model runtimes (<i>e.g., Ollama, LM Studio, Jan</i>) • Model size, parameters and quantization basics • Hardware considerations for local inference (<i>RAM, VRAM, CPU, GPU</i>) • Role of system prompts and prompt engineering • Overview of security-specialized open-weight models (<i>e.g., Foundation-Sec-8B</i>) Skills • Prompt engineering skills • Documentation skills • Communication skills • Observation skills • Analytical skills • Planning skills • Problem solving skill Attitude, safety and environmental concern • Being responsible while locally deploying AI models • Being aware of risks of unsecured local models (data leakage) • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Encouraging inclusive participations • Being vigilant and patient while generating outputs with help of AI • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation C2.03 Applying data analytics to identify patterns, indicators and anomalies Knowledge • Introduction to Python for security analytics • Introduction to Data analytics tools (<i>PowerBI, Tableau, ELK</i>) • Python programming fundamentals — pandas DataFrames, groupby, filter, merge, value_counts • Frequency analysis and threshold-based anomaly detection concepts • Time-series analysis and event clustering concepts • Relationship between manual analytics techniques and AI/ML detection models Skills • Record management skills • ICT skills • Communication skills • Observation skills
--	---

	• Analytical skills • Planning skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Attention to detail in anomaly detection • Being responsible in in avoiding misinterpretation of data • Having integrity while reporting findings • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Having sense of ownership and accountability • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation C2.04 Interpreting analysis results to support cybersecurity tasks <i>Knowledge</i> • MITRE ATT&CK kill chain tactic progression and technique taxonomy • CISA KEV catalog structure and application as a threat intelligence reference <i>Skills</i> • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Being responsible in interpreting threat intelligence correctly • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Being vigilant and patient • Having work ethics and integrity • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation C2.05 Predicting potential security issues using analyzed data <i>Knowledge</i> • Introduction to AI prediction models (<i>K-means clustering Regression analysis, time series analysis, Decision trees, etc</i>)
--	--

	<i>Skills</i> • Record management skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Being aware of uncertainty in AI predictions • Being responsible in using predictions for decision-making • Ethical consideration of prediction impact • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Having sense of ownership and accountability • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation C2.06 Validating effectiveness of security controls using analysis results <i>Knowledge</i> • MITRE D3FEND defensive technique framework <i>Skills</i> • Record management skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Being responsible in validating security control effectiveness • Being accountable while reporting system weaknesses • Having growth mindset • Effective time management • Being efficient in using resources • Encouraging inclusive participations • Having sense of ownership and accountability • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation
--	--

Learning Conditions	Learning Materials • Competency Based Learning Materials (CBLM) • Hand-outs • Audio Visuals • Reference books • Manuals Learning Facilities and infrastructure • Classroom with adequate facilities • Information Technology (IT) lab • Library • Workshop Materials • Pen, pencil and paper Software • Spreadsheet software, documentation tools, access to security tools and monitoring consoles, local model runtime (<i>eg. Ollama, LM studio, Jan</i>), open-weight AI model (<i>general-purpose or security-specialized</i>), python with relevant libraries, matplotlib, pandas & relevant analysis tools, data analytics tools (<i>Eg. PowerBI, Tableau, ELK</i>), Wireshark, Wazuh dashboard and openVAS Equipment • Computer with internet connectivity, workstation with sufficient RAM/VRAM and disk space with internet connectivity (<i>for initial model download</i>) PPE • Working dress and safety boot
Instructional Methodologies	The trainer shall use <i>inter alia</i>, the following instructional methods: • Lecture • Interactive discussion • Demonstration • Industrial visit/training • Guided practice • Group practice with project-based learning • Individual practice with problem-based learning • Universal Design of Learning (UDL)
Method of Assessment	The trainer shall use <i>inter alia</i>, the following assessment methods: • Practical observation • Oral/viva-voce • Written test • Assignment • Project work

Module Title	Apply Artificial Intelligence in Cybersecurity Operations		
Module Code	2529-L4-M3		
Learning Outcome 3	Apply Adversarial AI Techniques		
Duration	Theory: 49 hours	Practical: 112 hours	Total: 161 hours
Assessment Criteria	- Basic weaknesses in AI-based systems identified as per the job requirement following standard procedure - AI solutions are deployed as per the job requirement following standard procedure - AI solutions are applied as per the job requirement following standard procedure - AI solutions are verified against expected outcomes as per the job requirement following standard procedure		
Content	C3.01 Identifying basic weakness in AI-based systems Knowledge - Types of AI weaknesses (<i>bias, hallucination, data leakage, access issues, model prompt injection</i>) - Introduction to AI security concepts - Introduction to AI reliability issues (<i>training data limitations, knowledge cutoff</i>) Skills - Interpreting AI system components and architecture - ICT skills - Communication skills - Observation skills - Analytical skills - Planning skills - Numeracy skills - Problem solving skill Attitude, safety and environmental concern - Curiosity without misuse - Being responsible in identifying AI weaknesses without misuse - Having respect for system boundaries and permissions - Being aware of impact of AI vulnerabilities - Effective time management - Being efficient in using resources - Encouraging inclusive participations - Ensuring appropriate use of PPE - Ensuring proper disposal of waste - Ensuring to follow environmental rules and regulations - Ensuring to follow OHS rules and regulation C3.02 Applying simple adversarial techniques to test systems Knowledge - Introduction to attack surfaces and threat simulation - Responsible AI concepts		

	<i>Skills</i> • Adversarial inputs Designing Skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Numeracy skills • Problem solving skill • Coaching skills <i>Attitude, safety and environmental concern</i> • Adhering to authorized testing scope • Ethical responsibility in simulating attacks • Effective time management • Being efficient in using resources • Being vigilant and patient • Having sense of ownership and accountability • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation C3.03 Conduct basic attack simulations on AI models <i>Knowledge</i> • Concept of adversarial machine learning and AI attack simulation • Introduction to adversarial tools such as ✓ Adversarial Robustness Toolbox (ART) ✓ CleverHans • Importance of sandbox/cloned environments for testing <i>Skills</i> • Designing structured attack scenarios • Using AI security testing tools (basic level) • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Numeracy skills • Problem solving skill <i>Attitude, safety and environmental concern</i> • Curiosity without misuse • Being responsible to conduct testing in sandbox environments only • Being aware of risks of adversarial experimentation • Effective time management
--	--

	• Being efficient in using resources • Being vigilant and patient • Proper handling of system • Having sense of ownership and accountability • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation C3.04 Recommending improvements to strengthen AI system security Knowledge • Types of AI responses (<i>expected, unexpected, error, refusal</i>) • Methods for recording and organizing test results (<i>logs, screenshots, transcripts</i>) • Principles of secure AI system design and continuous improvement • Importance of clear procedural recommendations Skills • AI skills • ICT skills • Communication skills • Observation skills • Analytical skills • Planning skills • Problem solving skill Attitude, safety and environmental concern • Having integrity in reporting AI vulnerabilities • Being responsible in strengthening system security • Effective time management • Being efficient in using resources • Being vigilant and patient • Proper handling of system • Having sense of ownership and accountability • Ensuring appropriate use of PPE • Ensuring proper disposal of waste • Ensuring to follow environmental rules and regulations • Ensuring to follow OHS rules and regulation
Learning Conditions	Learning Materials • Competency Based Learning Materials (CBLM) • Hand-outs • Audio Visuals • Reference books • Manuals Learning Facilities and infrastructure • Classroom with adequate facilities

	• Information Technology (IT) lab • Library Materials • Pen, pencil and paper Software • AI/ML integrated test system, diagramming tools, basic note-taking tools, AI testing interface or chatbot system, LLM playground or testing interface, test datasets or sample inputs, sandbox or cloned AI environment and adversarial tools (<i>e.g., Adversarial Robustness Toolbox (ART), CleverHans</i>) Equipment • Computer with internet connectivity and high-end server PPE • Working dress and safety boot
Instructional Methodologies	The trainer shall use <i>inter alia</i>, the following instructional methods: • Lecture • Interactive discussion • Demonstration • Industrial visit/training • Guided practice • Group practice with project-based learning • Individual practice with problem-based learning • Universal Design of Learning (UDL)
Method of Assessment	The trainer shall use <i>inter alia</i>, the following assessment methods: • Practical observation • Oral/viva-voce • Written test • Assignment • Project work

ANNEXES

Annex I: Time Distribution Sheet

Cybersecurity Technologist					
Module Title	Learning outcomes	Tasks	Theory (Hours)	Practical (Hours)	Total (hours)
A: Manage network security	A1: Perform network security need assessment	A1.00 Introductory Knowledge	42	0	42
		A1.01 Develop organizations ICT assets inventory	7	14	21
		A1.02 Determine threats and vulnerabilities	7	21	28
		A1.03 Perform security assessment	7	21	28
		A1.04 Analyze security assessment report	7	14	21
	Sub Total Duration		70	70	140
	A2: Apply network security controls	A2.01 Configure home network	14	56	70
		A2.02 Configure VLAN	7	14	21
		A2.03 Configure VPN	7	21	28
		A2.04 Configure firewall and IDS	7	28	35
	Sub Total Duration		35	119	154
	A3: Manage and monitor network security	A3.01 Identify network monitoring tools	14	21	35
		A3.02 Deploy network security monitoring tools	14	56	70
		A3.03 Analyze network security events	14	56	70
		A3.04 Perform incident response	14	14	28
	Sub Total Duration		56	147	203
	Total duration (A)		161	336	497
B: Manage system security	B1: Manage system access and controls	B1.01 Manage users	3	4	7
		B1.02 Manage groups	3	4	7
		B1.03 Manage file permissions	7	7	14

		B1.04 Implement role-based access control	7	14	21
	Sub Total Duration		20	29	49
	B2: Perform system hardening	B2.01 Harden operating system	21	28	49
		B2.02 Harden web server	14	21	35
		B2.03 Harden database server	14	21	35
	Sub Total Duration		49	70	119
	B3: Perform application and web security	B3.01 Perform vulnerability assessment	21	56	77
		B3.02 Perform penetration testing	33	100	133
		B3.03 Prepare recommendation report	7	14	21
	Sub Total Duration		61	170	231
	B4: Maintain information security	B4.01 Classify information and data	7	21	28
		B4.02 Maintain data confidentiality	7	21	28
		B4.03 Maintain data integrity	7	21	28
		B4.04 Perform data backup and recovery	7	28	35
	Sub Total Duration		28	91	119
	Total duration (B)		158	360	518
C: Apply Artificial Intelligence in Cybersecurity Operations	C1: Implement AI solutions for Cybersecurity	C1.01 Identify cybersecurity tasks that can be optimized using appropriate AI tools	28	14	42
		C1.02 Deploy AI solutions	7	28	35
		C1.03 Apply AI solutions to solve cyber security tasks	7	28	35
		C1.04 Verify AI solution performance against expected outcomes	7	14	21
	Sub Total Duration		49	84	133
	C2: Analyze Security Data	C2.01 Identify relevant cybersecurity data sources	14	21	35
		C2.02 Deploy model locally	14	28	42
		C2.03 Apply data analytics to identify patterns, indicators and anomalies	56	56	112
		C2.04 Interpret analysis results to support cybersecurity tasks	7	28	35

		C2.05 Predict potential security issues using analyzed data	21	21	42
		C2.06 Validate effectiveness of security controls using analysis results	7	14	21
	Sub Total Duration		119	168	287
	C3: Apply Adversarial AI Techniques	C3.01 Identify basic weaknesses in AI-based systems	7	21	28
		C3.02 Apply simple adversarial techniques to test systems	14	21	35
		C3.03 Conduct basic attack simulations on AI models	21	56	77
		C3.04 Recommend improvements to strengthen AI system security	7	14	21
	Sub Total Duration		49	112	161
	Total duration (C)		217	364	581
	Grand Total		536	1060	1596

Annex II: Module Recognition

This is to verify that

Mr/Ms.....

has completed module on

.....

Covering following learning outcomes:

1.
2.
3.

Instructor:

Head of the Department:

.....

.....

Signature:

Signature:

Date: / / (dd/mm/yyyy)

Date: / /(dd/mm/yyyy)

Head of the Institute:

Trained Assessor (Institute)/Exam OC:

.....

.....

Signature:

Signature:

Date: .../ .../ (dd/mm/yyyy)

Date://(dd/mm/yyyy)

Annex IV: Lesson Plan
Lesson Plan

Course Title:		NC Level:
Module Code:		Duration:
Module Title:		
Learning Outcome:		
Skill/Task/Topic:		
Terminal Performance Objective:		
<i>(Note: Write narrative statement extracted from TPO of Task Sheet)</i>		
Enabling Objectives (Related knowledge):		
<i>By the end of the lesson learners will be able to:</i>		
i) ii) iii)		
What (Content/Activity)	Who (T/L)	How (Methods/ Media) Duration (Min.) Questions
Introduction: Main body Conclusion		
Projects/Problems:		

Instructional Resources Plan				
Skills/Task/Topic:				
No. of Trainees:				
Sl. No.:	Instructional materials/resources	Specifications	Qty.	Remarks
Prepared by :		Signature	Date:	
Revised by:		Signature	Date:	
Approved by:		Signature	Date:	

Task sheet

TS-1/4: Practical Plan

Course Title:		N C Level:	
Module code:		Duration:	
Module Title			
Learning outcome			
Skills/Task Title:		Task no:	
Terminal Performance Objective: <i>Given:</i> <i>Cue:</i> <i>Who:</i> <i>What:</i> <i>Within:</i> <i>How well:</i> - - -			
Enabling Objectives (Related Skills): <i>By the end of a lesson, the learners will be able to:</i> i) ii) iii) iv)			
Activities	Who (T/L)	How (methods/ media)	Duration

Project/Assignment:**TS-2/4: Tool and Equipment required:**

<i>Sl no.</i>	<i>Particulars</i>	<i>Specifications</i>	<i>Qty.</i>	<i>Remarks</i>

Training Materials required:

<i>Sl no.</i>	<i>Particulars</i>	<i>Specifications</i>	<i>Qty.</i>	<i>Rate</i>	<i>Amount</i>	<i>Remarks</i>

TS-3/4: Performance Guide**Skill/Task:****Date:**

Directions: Use the following performances criteria to rate the learner. Check YES/NO to indicate whether the learner performed each step as indicated or not?

Sl. No:	Steps	Yes	No

Note: Critical steps: All * marked steps should be carried out very carefully. For a quality performance guide, all items should be checked "YES"			

TS-4/4: Instruction and Drawing

General Instructions for Trainees

- i)
- ii)
- iii)
- iv)

Drawing (if any)

Safety Precaution

- i)
- ii)

iii)

Prepared by :	Signature	Date:
Revised By:	Signature	Date:
Approved by :	Signature	Date:

Annex V: Course Plan
Institutes letter head and Logo

(Trade)YEAR PLAN- _____ **Semester** _____ **(Year)**

Trade: NC Level:			Schedule																																Total Hours												
Module Code	Module Title	Learning Outcome	Feb.				March				April				May				June				July				Aug.				Sept					Oct.				Nov.							
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4		1	2	3	4								
OJT																																															
Assessment and Certification																																															

Prepared by:

Verified & Approved by:

Date:

Monthly/Weekly Plan

Month: Trade: Trainer:

Week	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Week 01							
Week 02							
Week 03							
Week 04							
Week 05							

Developed by: Approved by:

Date



For more information please contact:

Technical Trainers Training and Resource Center (TTTRC), DWPSD

Email: dwpsd@moesd.gov.bt/tttrd@moesd.gov.bt