REPUBLIC OF KENYA

COMPETENCY BASED MODULAR CURRICULUM

FOR

CYBER SECURITY

KNQF LEVEL 6

(CYCLE 3)

PROGRAMME ISCED CODE: 0612554A

TVET CDACC
P.O. BOX 15745-00100
NAIROBI

Council Secretary/CEO
TVET Curriculum Development, Assessment and Certification Council
P.O. Box 15745–00100
Nairobi, Kenya
Email: info@tvetcdacc.go.ke

FOREWORD

The provision of quality education and training is fundamental to the Government's overall strategy for social and economic development. Quality education and training contribute to the achievement of Kenya's development blueprint and sustainable development goals.

Reforms in the education sector are necessary to achieve Kenya Vision 2030 and meet the provisions of the Constitution of Kenya 2010. The education sector had to be aligned to the Constitution, and this resulted in the formulation of the Policy Framework for Reforming Education and Training in Kenya (Sessional Paper No. 14 of 2012). A key feature of this policy is the radical change in the design and delivery of TVET training. This policy document requires that training in TVET be competency-based, curriculum development be industry-led, certification be based on demonstration of competence, and the mode of delivery allow for multiple entry and exit in TVET programmes.

These reforms demand that Industry takes a leading role in curriculum development to ensure the curriculum addresses its competence needs. It is against this background that this curriculum has been developed. For trainees to build their skills on foundational hands-on activities of the occupation, units of learning are grouped in modules. This has eliminated duplication of content and streamlined exemptions based on skills acquired as a trainee progresses in the up-skilling process, while at the same time allowing trainees to be employable in the shortest time possible through the acquisition of part qualifications.

It is my conviction that this curriculum will play a great role in developing competent human resources for the Cyber Security Sector's growth and development.

PRINCIPAL SECRETARY
STATE DEPARTMENT FOR TVET
MINISTRY OF EDUCATION

PREFACE

Kenya Vision 2030 aims to transform Kenya into a newly industrializing middle-income country, providing high-quality life to all its citizens by the year 2030. Kenya intends to create globally competitive and adaptive human resource base to meet the requirements of a rapidly industrializing economy through lifelong education and training. TVET has a responsibility to facilitate the process of inculcating knowledge, skills, and worker behaviour necessary for catapulting the nation to a globally competitive country, hence the paradigm shift to embrace Competency-Based Education and Training (CBET).

CAP 210A and Sessional Paper No. 1 of 2019 on Reforming Education and Training in Kenya for Sustainable Development emphasized the need to reform curriculum development, assessment, and certification. This called for a shift to CBET to address the mismatch between skills acquired through training and skills needed by industry, as well as increase the global competitiveness of the Kenyan labour force.

This curriculum has been developed in adherence to the Kenya National Qualifications Framework and CBETA standards and guidelines. The curriculum is designed and organized into Units of Learning with Learning Outcomes, suggested delivery methods, learning resources, and methods of assessing the trainee's achievement. In addition, the units of learning have been grouped in modules to concretize the skills acquisition process and streamline upskilling.

I am grateful to all expert trainers and everyone who played a role in translating the Occupational Standards into this competency-based modular curriculum.

CHAIRMAN
TVET CDACC

ACKNOWLEDGMENT

This curriculum has been designed for competency-based training and has independent units of learning that allow the trainee flexibility in entry and exit. In developing the curriculum, significant involvement and support were received from expert trainers, institutions and organizations.

I recognize with appreciation the role of the ICT National Sector Skills Committee (NSSC) in ensuring that competencies required by the industry are addressed in the curriculum. I also thank all stakeholders in the ICT sector for their valuable input and everyone who participated in developing this curriculum.

I am convinced that this curriculum will go a long way in ensuring that individuals aspiring to work in the ICT sector acquire competencies to perform their work more efficiently and effectively.

COUNCIL SECRETARY/CEO
TVET CDACC

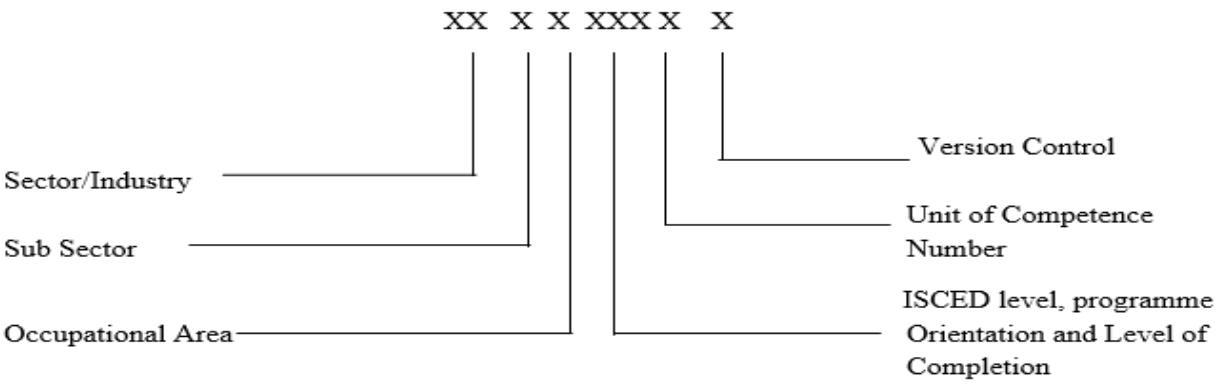
TABLE OF CONTENTS

ABBREVIATIONS

ICT	Information Communication Technology
IS	Information System
ISP	Information Security Policy
KCSE	Kenya Certificate of Secondary Education
KNQA	Kenya National Qualification Authority
KNQF	Kenya National Qualification Framework
LAN	Local Area Network
WLAN	Wireless Local Area Network
MIS	Management Information System
PAN	Personal Area Network
SOP	Sum of Product
POST	Power on Self-Test
PPE	Personal Protective Equipment
RAM	Random Access Memory
SDLC	System Development life cycle
TVET	Technical and Vocational Education and Training
WAN	Wide Area Network
DOM	Document Object Model
DBMS	Database Management System
RJ45	Registered Jack 45
UTP	Unshielded Twisted Pair
GNS3	Graphical Network Simulator 3
AIDE	Advanced Intrusion Detection Environment
MYSQL	My Structured Query Language

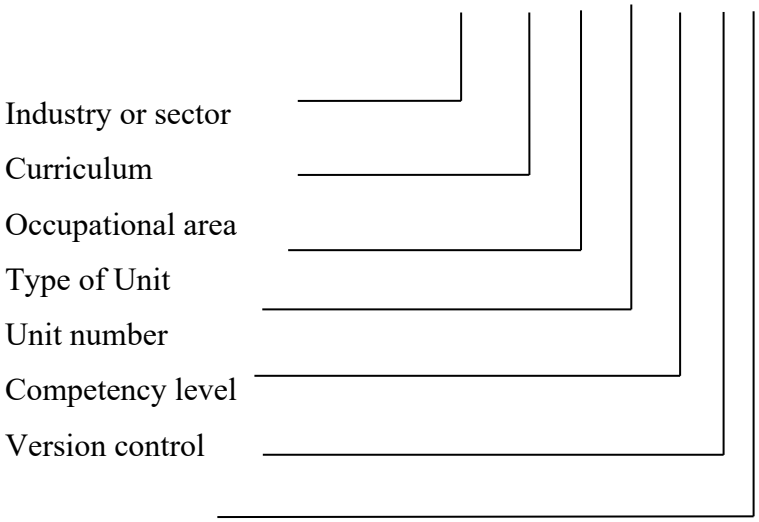
KEY TO UNIT CODE

KEY TO ISCED UNIT CODE



KEY TO TVET CDACC UNIT CODE

SEC/CU/CS/BC/01/5/MA



COURSE OVERVIEW

Cyber Security Level 6 Curriculum consists of competencies that an individual must possess to enable him or her be certified as a Cyber Security Technician. It involves Performing Computer Operations, Computer Repair and Maintenance, Computer Networking, Database Security, Install and Configure Linux, Perform Website Design and Development, Secure Software Application, Security Assessment and Testing.

Summary of Units of Learning

ISCED Unit Code	TVE CDACC Unit Code	Unit of Learning Title	Duration in Hours	Credit Factor
MODULE I				
0612554 01A	SEC/CU/CS/CR/01/5/MA	Perform Computer Operations	150	15
0612554 02A	SEC/CU/CS/CR/02/5/MA	Perform Computer Repair and Maintenance	200	20
0031 441 01A	SEC/CU/CS/BC/01/5/MA	Communication Skills	40	4
SUB TOTAL			**390**	**39**
MODULE II				
0612554 03A	SEC/CU/CS/CR/03/5/MA	Perform Computer Networking	200	20
0612554 04A	SEC/CU/CS/CR/04/5/MA	Secure Databases	120	12
0417 441 02A	SEC/CU/CS/BC/02/5/MA	Work Ethics and Practices	40	4
SUB TOTAL			**360**	**36**
MODULE III				
0612554 05A	SEC/CU/CS/CR/05/5/MA	Install and Configure Linux	150	15
0612554 06A	SEC/CU/CS/CR/06/5/MA	Secure Software Application	150	15
0413 441 03A	SEC/CU/CS/BC/03/5/MA	Entrepreneurial Skills	40	4
SUB TOTAL			**340**	**34**
MODULE IV				
0612554 07A	SEC/CU/CS/CR/07/5/MA	Perform Website Design and Development	200	20
0612554 08A	SEC/CU/CS/CR/08/5/MA	Conduct Security Assessment and Testing,	150	15

0612554 09A	SEC/CU/CS/CU/01/5/MA	Demonstrate understanding of Cybersecurity Laws, Policies and Regulations	120	12
SUB TOTAL			**470**	**47**
MODULE V				
0612554 10A	SEC/CU/CS/CR/01/6/MA	Build Secure Networks	120	12
0612554 11A	SEC/CU/CS/CR/02/6/MA	Manage Security Operations	160	16
0612554 12A	SEC/CU/CS/CR/03/6/MA	Develop Computer Software	200	20
SUB TOTAL			**480**	**48**
	SEC/CU/CS/CR/06/6/MA	**INDUSTRY TRAINING**	**480**	**48**
GRAND TOTAL			**2520**	**252**

Trainee Entry Requirements

An individual entering this course should have any of the following minimum requirements:

a) Kenya Certificate of Secondary Education (KCSE) mean grade C-(minus)

Or

b) Cyber Security or related level 5 certificate

or

c) Equivalent qualification as determined by TVETA

Trainer Qualification

Qualifications of a trainer for this course include:

a) Possession of a higher qualification than Cyber security Level 6 or its equivalent in a trade area related to this course.
b) License by TVETA.

Industry Training

An individual enrolled in this course will be required to undergo Industry training for a minimum period of 480 hours in Cyber Security Sector. The industrial training may be taken after completion of all units for those pursuing the full qualification or be distributed equally in each unit for those pursuing part qualification. In the case of dual training model, industrial training shall be as guided by the dual training policy.

Assessment

The course shall be assessed formatively and summatively:

1. During formative assessment all performance criteria shall be assessed based on performance criteria weighting.
2. Number of formative assessments shall minimally be equal to the number of elements in a unit of competency.
3. During summative assessment basic and common units may be integrated in the core units or assessed as discrete units.
4. Theoretical and practical weighting for each unit of learning shall be as follows:
    i. 30-70 for units in module I and module IV
    ii. 40-60 for units in modules V and VI
5. Formative and summative assessments shall be weighted at 60% and 40% respectively in the overall unit of learning score

    For a candidate to be declared competent in a unit of competency, the candidate must meet the following conditions:

    i. Obtained at least 40% in theory assessment in formative and summative assessments.
    ii. Obtained at least 60% in practical assessment in formative and summative assessment where applicable.
    iii. Obtained at least 50% in the weighted results between formative assessment and summative assessment where the former constitutes 60% and the latter 40% of the overall score.
6. Assessment performance rating for each unit of competency shall be as follows:

MARKS	COMPETENCE RATING
80 -100	Attained Mastery
65 - 79	Proficient
50 - 64	Competent
49 and below	Not Yet Competent
Y	Assessment Malpractice/irregularities

7. Assessment for Recognition of Prior Learning (RPL) may lead to award of part and/or full qualification.

Certification

A candidate will be issued with a Certificate of Competency upon demonstration of competence in a core Unit of Competency. To be issued with Kenya National TVET Certificate in Cyber Security Level 6, the candidate must demonstrate competence in all the Units of Competency as given in the qualification pack. Statement of Attainment certificate may be awarded upon demonstration of competence in certifiable element within a unit.

These certificates will be issued by TVET CDACC

MODULE I

ISCED Unit Code	TVE CDACC Unit Code	Unit of Learning Title	Duration in Hours	Credit Factor
0612554 01A	SEC/CU/CS/CR/01/5/MA	Perform Computer Operations	150	15
0612554 02A	SEC/CU/CS/CR/02/5/MA	Perform Computer Repair and Maintenance	200	20
0031 441 01A	SEC/CU/CS/BC/01/5/MA	Communication Skills	40	4
Total hours			**390**	**39**

PERFORM COMPUTER OPERATIONS

ISCED UNIT CODE: 0612554 01A

TVET CDACC UNIT CODE: SEC/CU/CS/CR/01/5/MA

Relationship to Occupational Standards

This unit addresses the Unit of Competency: Perform Computer Operations

Duration of Unit: 150 hours

Unit Description

This unit covers the competencies required to perform computer operations. It involves processing computerized word documents, manipulating computerized spreadsheets, maintaining computerized databases, manipulating presentation slides, manipulating graphic application and performing online collaboration.

Summary of Learning Outcomes

Learning Outcomes	Durations (Hours)
1. Process computerized word document	30
2. Manipulate computerized spreadsheet	30
3. Maintain computerized database	30
4. Prepare PowerPoint presentation	20
5. Manipulate graphic application	25
6. Perform online collaboration	15
Total Hours	**150**

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Process computerized word document	1.1 Ergonomics risk factors 1.2 Operating Computer devices 1.2.1 Meaning and importance of computer	● Practical assessment ● Simulations ● Project

	1.2.2 Functions and Uses of Computers 1.2.3 Classification of computers 1.2.4 Components of a computer system 1.2.5 Computer Hardware 1.2.6 Procedure for turning/off a computer 1.2.7 Desktop Customization 1.2.8 File and Files Management using an operating system 1.2.9 Computer external devices management 1.3 Creation of computerized word document 1.3.1 Introduction to word document 1.3.2 Types of word processors 1.3.3 Creating word document 1.4 Editing and formatting word document 1.3.4 Word document editing features 1.3.5 Word document formatting features 1.3.6 Enhancing productivity 1.5 Mail merge 1.5.1 Mail merge preparation 1.5.2 Mail merge output 1.6 Printing of computerized word document 1.6.1 Print setup 1.6.2 Printing	● Observation Checklist ● Product Checklist ● Written assessment ● Portfolio of evidence

2. Manipulate computerized spreadsheet	2.1 Creation of Computerized spreadsheet workbook 2.1.1 Spreadsheet concepts 2.1.2 Cell referencing 2.1.3 Spreadsheet editing features 2.1.4 Data manipulation in spreadsheets 2.1.5 Formulas and functions 2.2 Computerized spreadsheet worksheet formatting 2.2.1 Spreadsheet formatting features 2.2.2 Data presentation 2.3 Computerized spreadsheet workbook printing 2.3.1 Print setup 2.3.2 Printing	● Practical assessment ● Simulations ● Project ● Observation Checklist ● Product Checklist ● Written assessment ● Portfolio of evidence
3. Maintain computerised database	3.1 Computerised database user requirements collection 3.1.1 Understand database 3.1.2 Collection of User requirements 3.2 Design Computerised database schema 3.2.1 Creating database models 3.3 Creation of Computerised database objects 3.3.1 Database Objects 3.4 Data manipulation 3.4.1 Inserting records 3.4.2 Retrieving records	● Practical assessment ● Simulations ● Project ● Observation Checklist ● Product Checklist ● Written assessment ● Portfolio of evidence

	3.4.3 Deleting records 3.4.4 Updating record 3.4.5 Printing database objects	
4. Manipulate presentation slides	4.1 Collection of Presentation requirements 4.2.1 Definition of terms 4.2.2 Presentation requirements 4.2.3 Types of presentation software 4.2.4 Elements of presentation window 4.2.5 Manipulating presentations 4.2.6 Working with presentations 4.2 Presentation layout set up 4.3 Creation of a Slide 4.3.1 Slide views 4.3.2 Slide designs 4.3.3 Slide transition 4.4 Manipulation of a slide 4.4.1 Adding data/text to a slide 4.4.2 Slide animation 4.4.3 Formatting data/text 4.4.4 Move/copy/delete a slide 4.4.5 Inserting header and footer 4.4.6 Presentation objects 4.4.7 Print setup	● Practical assessment ● Simulations ● Project ● Observation Checklist ● Product Checklist ● Written assessment ● Portfolio of evidence

5. Manipulate graphic application	5.1 Collecting graphic design requirements 5.1.1 Definition of terms 5.1.2 Graphic application requirements 5.1.3 Types of graphic application software 5.1.4 Types of publications designs 5.1.5 Elements of Graphic application window 5.2 Creation of graphic design 5.2.1 Perform basic tasks using graphic application software 5.2.2 Add content to a publication 5.2.3 Edit content to a publication 5.2.4 Format text and paragraphs in a publication 5.2.5 Page formatting in a publication 5.2.6 Work with graphics objects in a publication 5.3 Publishing of graphic design 5.3.1 Prepare a publication 5.3.2 Print setup 5.3.3 Printing publication	● Practical assessment ● Simulations ● Project ● Observation Checklist ● Product Checklist ● Written assessment ● Portfolio of evidence
6. Perform Online Collaboration	6.1 Identification of Online collaboration tools 6.1.1 Definition of online	● Practical assessment ● Simulations

	collaboration 6.1.2 Importance of online collaboration 6.1.3 Online collaboration tools 6.2 Online collaboration preparation 6.2.1 Collaboration concepts 6.2.2 Common setup features 6.2.3 Preparation for online collaboration 6.3 Application of online collaborative tools 6.3.1 Using online collaborative tools 6.4 Demonstrating Mobile collaborations	● Project ● Observation Checklist ● Product Checklist ● Written assessment ● Portfolio of evidence

Suggested Delivery Methods

- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos
- Group discussions
- Facilitation using active learning strategies

Recommended Resources for 25 trainees

S/No.	Category/Item	Description/Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			
1	Textbooks		5 pcs	5:1
2	Installation manuals		5 pcs	5:1

3	Flip Charts		5 pcs	5:1
4	PowerPoint presentations	For trainer's use		
5	Magazines/brochures/business cards			
B	**Learning Facilities Infrastructure**			
6	Lecture/theory room		1	25:1
7	Laboratory		1	25:1
C	**Consumable Materials**			
8	Printing papers		1 ream	1:20
9	Foolscaps		1 ream	
10	Toners/cartridges		2 pcs	13:1
11	Assorted colour whiteboard markers			
D	**Tools and Equipment**			
12	Computers		25 pcs	1:1
13	Projector		1 pc	25:1
14	Printers		2 pcs	1:13
16	Whiteboard		1 pc	25:1
17	Flash drives		5 pcs	5:1
18	1 External Hard drive		1 pc	25:1
19	Application software suite		5 pc	

PERFORM COMPUTER REPAIR AND MAINTENANCE

ISCED UNIT CODE: 0612554 02A

TVET CDACC UNIT CODE: SEC/CU/CS/CR/02/5/MA

Relationship to Occupational Standards

This unit addresses the unit of competency: Perform computer repair and maintenance

Duration of Unit: 200 Hours

Unit Description

This unit covers the competencies required for performing computer repair and maintenance. It involves performing computer troubleshooting, repairing faulty components, testing computer component functionality and performing computer maintenance.

Summary of Learning Outcomes

Learning Outcomes	Durations (Hours)
1. Perform computer troubleshooting	50
2. Repair faulty components.	60
3. Test computer component functionality	60
4. Perform computer maintenance	30
Total Hours	**200**

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Perform computer troubleshooting	1.1. User data assessment 1.1.1. Introduction to computer troubleshooting 1.2. Computer problems identification 1.2.1. User data analysis, diagnosis and resolving 1.3. Determining solution to the problem	● Practical assessment ● Project ● Observation Checklist ● Product Checklist

	1.3.1. Computer hardware faults remedies	● Written assessment ● Portfolio of evidence
2. Repair faulty components.	2.1 Selection of computer components for replacement 2.4.1 Computer hardware components 2.2 Assembly of tools for repairing or replacing 2.4.2 Computer repair and maintenance tools 2.3 Observation of Safety procedures 2.4.3 Safety measures and procedures 2.4 Repair and replacing computer components 2.4.4 Repair and replacing components Instruction manuals 2.4.5 Computer components disassembly process 2.4.6 Reassembling repaired or replaced computer components 2.5 Disposing faulty or obsolete computer hardware components 2.5.1 Pollution	● Practical assessment ● Project ● Observation Checklist ● Product Checklist ● Written assessment ● Portfolio of evidence
3. Test computer component functionality	3.1 Performing POST test on computer 3.2 Evaluation of test Results 3.3 Generation of test Results report	● Practical assessment ● Project ● Observation Checklist ● Product Checklist ● Written

		assessment ● Portfolio of evidence
4. Perform computer maintenance	4.1 Computer maintenance scheduling 4.1.1 Introduction to computer maintenance 4.1.2 Types of computer maintenance 4.2 Performing computer maintenance 4.2.1 Computer maintenance techniques 4.2.2 Computer maintenance utilities 4.2 Computer maintenance report 4.2.3 Importance of computer maintenance report 4.2.4 Components of computer maintenance report	● Practical assessment ● Project ● Observation Checklist ● Product Checklist ● Written assessment ● Portfolio of evidence

Suggested Delivery Methods

- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos
- Field trips
- On-job-training
- Group discussions

Recommended Resources for 25 trainees

S/No.	Category/Item	Description/Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			
1	Textbooks		2 pcs	13:1
2	Installation manuals		5 pcs	5:1
3	Flip Charts		5 pcs	5:1

4	PowerPoint presentations	For trainer's use		
B	**Learning Facilities Infrastructure**			
5	Lecture/theory room		1	25:1
6	Laboratory		1	25:1
7	Internet Connection			
C	**Consumable Materials**			
8	Printing papers		1 ream	1:20
9	Foolscaps		1 ream	1:20
10	Toners/cartridges		2 pcs	13:1
11	Assorted colour whiteboard markers	For trainer's use		
D	**Tools and Equipment**			
12	Computers		25 pcs	1:1
13	Projector		1 pc	25:1
14	Printers		2 pcs	13:1
16	Whiteboard		1 pc	25:1
17	Flash drives		5 pcs	5:1
18	1 External Hard drive		1 pc	25:1
19	Application software suite		9 pc	3:1
20	Signal Testers		5 pc	5:1
21	Antistatic gloves		25 pairs	1:1

COMMUNICATION SKILLS

ISCED UNIT CODE: 0031 441 01A

TVET CDACC UNIT CODE: SEC/CU/CS/BC/01/5/MA

Duration of Unit: 40 hours

Relationship to Occupational Standards

This unit addresses the Unit of Competency: Apply Communication Skills

Unit Description

This unit covers the competencies required to apply communication skills. It involves applying communication channels, written, non-verbal, oral, and group communication skills.

Summary of Learning Outcomes

LEARNING OUTCOMES	DURATION (HOURS)
1. Apply communication channels.	5
2. Apply written communication skills.	10
3. Apply non-verbal skills.	10
4. Apply oral communication skills.	5
5. Apply group communication skills.	10
TOTAL	**40**

Learning Outcomes, Content, and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Apply communication channels.	1.1 Communication process 1.1.1 Principles of effective communication 1.2 Channels/medium/modes of communication 1.2.1 Factors to consider when	• Oral assessment • Written assessment • Observation • Portfolio of Evidence • Practical assessment

	selecting a channel of communication 1.2.2 Barriers to effective communication 1.3 Flow/patterns of communication 1.3.1 Sources of information 1.3.2 Organizational policies	• Third party report
2 Apply written communication skills	2.1 Types of written communication 2.2 Elements of communication 2.3 Organization requirements for written communication	• Oral assessment • Written assessment • Observation • Portfolio of Evidence • Practical assessment • Third party report
3 Apply non-verbal communication skills	3.1 Utilize body language and gestures 3.2 Apply body posture 3.3 Apply workplace dressing code	• Oral assessment • Written assessment • Observation • Portfolio of Evidence • Practical assessment • Third party report
4 Apply oral communication skills	4.1 Types of oral communication pathways 4.2 Effective questioning techniques 4.3 Workplace etiquette 4.4 Active listening	• Oral assessment • Written assessment • Observation • Portfolio of Evidence • Practical assessment • Third party report
5 Apply group discussion skills	5.1 Establishing rapport 5.2 Facilitating resolution of issues 5.3 Developing action plans 5.4 Group organization techniques 5.5 Turn-taking techniques 5.6 Conflict resolution techniques	• Oral assessment • Written assessment • Observation • Portfolio of Evidence • Practical assessment

	5.7 Team-work	

Suggested Methods of Instruction

- Roleplaying
- Simulation
- Field trips
- Viewing of related videos
- Demonstrations
- Online Training
- Group discussions.
- Instructor led facilitation using active learning strategies

Recommended Resources for 25 trainees

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			
1.	Textbooks		5 pcs	5:1
2.	PowerPoint presentations	For trainer's use		
3.	Assorted colour of whiteboard markers	For trainer's use		
4.	e-Didactics	For trainer's use		
5.	Flashcards			
6.	Flip charts			
7.	Whiteboard			
B	**Learning Facilities & infrastructure**			
8.	Lecture/theory room		1	25:1
9.	Consumable materials			
10.	Printing Papers		1 ream	1:20
12.	Toners		2 pcs	13:1
13.	Internet			
D	**Tools and Equipment**			
14.	Projectors		1	25:1

15.	Printers		4	6:1
16.	Computers/Smartphones		25 pcs	1:1

MODULE II

ISCED Unit Code	TVE CDACC Unit Code	Unit of Learning Title	Duration in Hours	Credit Factor
0612554 03A	SEC/CU/CS/CR/03/5/MA	Perform Computer Networking	200	20
0612554 04A	SEC/CU/CS/CR/04/5/MA	Secure Databases	120	12
0417 441 02A	SEC/CU/CS/BC/02/5/MA	Work Ethics and Practices	40	4
Total hours			**360**	**36**

PERFORM COMPUTER NETWORKING

ISCED UNIT CODE: 0612554 03A

TVET CDACC UNIT CODE: SEC/CU/CS/CR/03/5/MA

Relationship to Occupational Standards

This unit addresses the unit of competency: Perform computer networking

Duration of Unit: 200 hours

Unit Description

This unit covers the competencies required to perform computer networking. It involves identifying network types, configuring network devices, connecting network devices, monitoring network performance, documenting network report, training network users and maintaining of the network.

Summary of Learning Outcomes

Learning Outcomes	Durations (Hours)
1. Identify network type	20
2. Features and functions of computer networks	24
3. Network Protocols and Standards	30
4. Configure network devices	50
5. Maintain Network	46
6. Document network report	30
Total Hours	**200**

Learning Outcomes, Content and Suggested Assessment Methods:

Learning Outcome	Content	Suggested Assessment Methods
1. Identify network type	1.1. Meaning of terms 1.2. Network components 1.3. Network design and	• Written tests • Oral questioning • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	architecture 1.4. Types of network topology	• Observation
2. Features and Functions of Computer networks	2.1 Components of a network 2.2 Network types 2.3 Transmission media 2.4 Network topologies 2.5 Network standards	• Written tests • Oral questioning • Practical tests • Observation
3. Network Protocols and standards	3.1 Communication Protocols 3.1.1 OSI Model 3.1.2 TCP/IP Reference model 3.2 IPv4 Addressing 3.2.1 Classful addressing 3.2.2 Private vs Public 3.2.3 Classless addressing • Interdomain routing • Variable subnet masking 3.2.4 IPv6 Addressing 3.2.5 Subnetting IPv4 and IPv6	• Written tests • Oral questioning • Practical tests • Observation
4. Configure Network devices	4.1 Design a Local Area Network 4.1.1 Logical topology 4.1.2 Physical topology 4.2 Assigning IP Addresses 4.2.1 Static 4.2.2 Dynamic 4.3 Configure Routing protocols 4.3.1 Static 4.3.2 Dynamic 4.4 Perform network trouble	• Written tests • Oral questioning • Practical tests • Observation

Learning Outcome	Content	Suggested Assessment Methods
	shooting 4.4.1 Command line tools 4.4.2 Graphical tools	
5. Maintain Network	5.1 Importance of Network Maintenance 5.2 Types of Network Maintenance 5.2.1 Preventive 5.2.2 Corrective 5.2.3 Adaptive 5.3 Network Monitoring Tools 5.3.1 Wireshark 5.3.2 PRTG 5.3.3 NetFlow 5.3.4 SNMP 5.3.5 Syslog 5.4 Network scalability	• Written tests • Oral questioning • Practical tests • Observation
6. Document network report	6.1 Importance of Network Documentation 6.2 Types of Network Reports 6.3 Key Components of a Network Report 6.4 Writing an Executive Summary for Non-Technical Stakeholders	• Written tests • Oral questioning • Practical tests • Observation

Suggested Methods of Instructions

- Instructor led facilitation of theory
- Demonstration by trainer
- Practical work by trainee

- Viewing of related videos
- Group discussions

Recommended Resources for 25 trainees

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			
1.	Textbooks		13 pcs	13:1
2.	Installation manuals		5pcs	5:1
3.	Charts			
4.	PowerPoint presentations	For trainer's use		
B	**Learning Facilities & infrastructure**			
5.	Lecture/theory room		1	25:1
6.	Computer Laboratory		1	25:1
7.	Internet Connection			
C	Consumable materials			
8.	Printing papers		1 ream	1:20
9.	Toners		2 pcs	13:1
10.	Assorted colour of whiteboard markers			
D	**Tools and Equipment**			
1.	Computers		25 pcs	1:1
2.	Projector		1 pc	25:1
3.	Signal testers		5 pcs	5:1
4.	Header checker		25 pcs	1:1
5.	Crimping tools		25 pcs	1:1
6.	Cable tester		5 pcs	5:1
7.	Switches		5pcs	5:1
8.	Repeaters		5pcs	5:1
9.	Routers/modem		5pcs	5:1
10.	Network tool kit		25 pcs	1:1

11.	RJ45		300 pcs	1:10
12.	UTP Ethernet Cable		300 metres	1:10
13.	Antistatic gloves		25 pairs	1:1
14.	Wireshark 32/64-bit Latest version		25 pc	1:1
15.	Network simulation tools: -Cisco packet tracer or -GNS3		25 pc	1:1

SECURE DATABASES

ISCED UNIT CODE: 0612554 04A

TVET CDACC UNIT CODE: SEC/CU/CS/CR/04/5/MA

Relationship to Occupational Standards

This unit addresses the unit of competency: Secure databases

Duration of Unit: 120 hours

Unit Description

This unit covers the competencies required to secure databases. It involves identifying types of databases, identifying database threats and vulnerabilities, installing database patches, installing security management systems for database, monitoring database security, monitoring access control and managing database backups.

Summary of Learning Outcomes

Learning Outcomes	Durations (Hours)
1. Identify database management system	18
2. Design a database	22
3. Create a database	30
4. Implement database security measures	14
5. Monitor database security	20
6. Manage database backups	16
Total Hours	**120**

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Identify database management	1.1 Meaning of terms 1.2 Types of databases	• Written tests • Oral questioning

systems	1.3 Classification of databases 1.4 Database organization approaches 1.4.1 Hierarchical Database Approach 1.4.2 Network Database Approach 1.4.3 Relational Database Approach (RDBMS) 1.4.4 Object-Oriented Database Approach (OODBMS) 1.4.5 NoSQL Database Approach 1.5 Database design cycle	• Observation • Practical tests
2. Design a database	2.1 Design a relational database. 2.2 Create entity relationship 2.2.1 Connotations of entity relationship 2.2.2 Drawing ERDS 2.3 Perform Normalisation	• Written tests • Oral questioning • Observation • Practical tests
3. Create a database	3.1 Querying a database using MySQL 3.1.1 Identify categories of SQL statements. 3.1.2 Design SQL statements. 3.1.3 Design SQL Queries. 3.1.4 Use SQL statements to query a database.	•
4. Implement database security measures.	4.1 Identify database authorization techniques. 4.1.1 Role-Based Access Control (RBAC). 4.1.2 Attribute-Based Access Control (ABAC). 4.1.3 Least Privilege principle. 4.1.4 Multi factor authentication for database access. 4.2 Identify Concurrency Control	• Observation • Oral questioning • Practical tests • Written tests

	techniques 4.2.1 Locking mechanisms (e.g., exclusive locks, shared locks) 4.2.2 Two-phase locking. 4.2.3 Timestamp ordering. 4.2.4 Optimistic Concurrency Control.	
5. Monitor the database performance.	5.1 Identify database monitoring techniques 5.1.1 Transaction Auditing 5.1.2 Privileged User Auditing 5.1.3 Log-Based Auditing 5.1.4 Trigger-Based Auditing 5.2 Use tools to monitor database activities 5.3 Conduct Security Mitigation. 5.3.1 Review & Strengthen Access Controls 5.3.2 Contain and Neutralize Threats 5.3.3 Apply Security Patches & Updates	•
6. Manage database backups.	6.1 Understanding Backup Fundamentals 6.1.1 Backup types 6.1.2 Backup storage solutions 6.2 Conducting back up strategies 6.2.1 Backup frequency and retention policies. 6.2.2 Implement the backup rule 6.3 Configuring and Managing Backup Systems	• Written tests • Oral questioning • Observation • Practical tests

Suggested Methods of instructions

- Instructor led facilitation of theory
- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos

- Group discussions

Recommended Resources for 25 trainees

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			
1.	Textbooks		5 pcs	5:1
2.	PowerPoint presentations	For trainer's use		
3.	Assorted colour of whiteboard markers	For trainer's use		
4.	e-Didactics	For trainer's use		
5.	Flashcards			
6.	Flip charts			
7.	Whiteboard			
B	**Learning Facilities & infrastructure**			
8.	Lecture/theory room		1	25:1
9.	Consumable materials			
10.	Printing Papers		1 ream	1:20
12.	Toners		2 pcs	13:1
13.	Internet			
D	**Tools and Equipment**			
14.	Projectors		1	25:1
15.	Printers		4	6:1
16.	Computers.		25 pcs	1:1
17.	MySQL Database		25 pcs	1:1
	MySQL Workbench Community Edition		25 pcs	1:1

WORK ETHICS AND PRACTICES

ISCED UNIT CODE: 0417 441 02A

TVET CDACC UNIT CODE: SEC/CU/CS/BC/02/5/MA

Duration of Unit: 40 hours

Relationship to Occupational Standard

This unit addresses the Unit of Competency: Apply work ethics and practices.

Unit Description

This unit covers competencies required to effectively apply work ethics and practices. It involves applying self-management skills, promoting ethical work practices and values, promoting teamwork, maintaining professional and personal development, applying problem- solving and promoting customer care.

Summary of Learning Outcomes

Learning Outcomes	Durations (Hours)
1. Apply self-management skills	10
2. Promote ethical practices and values	10
3. Promote teamwork	5
4. Maintain professional and personal development	5
5. Apply problem-solving skills	5
6. Promote customer care.	5
Total Hours	**40**

Learning Outcomes, Content, and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Apply self-management skills	1.1 Self-awareness 1.2 Formulating personal vision, mission, and goals 1.3 Healthy lifestyle practices	• Oral questions • Written assessment • Observation • Portfolio of Evidence

	1.4 Strategies for overcoming work challenge 1.5 Emotional intelligence 1.6 Coping with Work Stress. 1.7 Assertiveness versus aggressiveness and passiveness 1.8 Developing and maintaining high self-esteem 1.9 Developing and maintaining positive self-image 1.10 Time management 1.11 Setting performance targets 1.12 Monitoring and evaluating performance targets	• Practical assessment • Third party report
2. Promote ethical practices and values	2.1 Integrity 2.2 Core Values, ethics and beliefs 2.3 Patriotism 2.4 Professionalism 2.5 Organizational codes of conduct 2.6 Industry policies and procedures	• Oral questions • Written assessment • Observation • Portfolio of Evidence • Practical assessment • Third party report
3. Promote teamwork	3.1 Types of teams 3.2 Team building 3.3 Individual responsibilities in a team 3.4 Determination of team roles and objectives 3.5 Team parameters and	• Oral questions • Written assessment • Observation • Portfolio of Evidence • Practical assessment • Third party report

	relationships 3.6 Benefits of teamwork 3.7 Qualities of a team player 3.8 Leading a team 3.9 Team performance and evaluation 3.10 Conflicts and conflict resolution 3.11 Gender and diversity mainstreaming 3.12 Developing Healthy workplace relationships 3.13 Adaptability and flexibility 3.14 Coaching and mentoring skills	
4. Maintain professional and personal development	4.1 Personal vs professional development and growth 4.2 Avenues for professional growth 4.3 Recognizing career advancement 4.4 Training and career opportunities 4.5 Assessing training needs 4.6 Mobilizing training resources 4.7 Licenses and certifications for professional growth and development 4.8 Pursuing personal and organizational goals 4.9 Managing work priorities and commitments	• Oral questions • Written assessment • Observation • Portfolio of Evidence • Practical assessment • Third party report

	4.10 Dynamism and on-the-job learning	
5. Apply problem-solving skills	5.1 Establishing rapport 5.2 Facilitating resolution of issues 5.3 Developing action plans 5.4 Group organization techniques 5.5 Turn-taking techniques 5.6 Conflict resolution techniques 5.7 Team-work	• Oral questions • Written assessment • Observation • Portfolio of Evidence • Practical assessment Third party report
6. Promote customer care	6.1 Identifying customer needs 6.2 Qualities of good customer service 6.3 Customer feedback methods 6.4 Resolving customer concerns 6.5 Customer outreach programs 6.6 Customer retention	• Oral assessment • Written assessment • Observation • Portfolio of Evidence • Practical assessment

Suggested Methods of Instruction

- Instructor lead facilitation of theory using active learning strategies.
- Demonstrations
- Simulation/Role play
- Group Discussion
- Presentations
- Projects
- Case studies
- Assignments

Recommended Resources for 25 Trainees

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			

1.	Textbooks		5 pcs	5:1
2.	PowerPoint presentations	For trainer's use		
3.	Assorted colour of whiteboard markers	For trainer's use	2 packets	
4.	e-Didactics	For trainer's use		
5.	Flashcards			
6.	Flip charts			
7.	Whiteboard			
B	**Learning Facilities & infrastructure**			
8.	Lecture/theory room		1	25:1
C	**Consumable materials**			
9.	Printing Papers		1 ream	1:20
10.	Toners		2 pcs	13:1
11.	Internet connection			
D	**Tools and Equipment**			
12.	Projectors		1	25:1
13.	Printers		4	6:1
14.	Computers/Mobile Phones		25 pcs	1:1

MODULE III

ISCED Unit Code	TVE CDACC Unit Code	Unit of Learning Title	Duration in Hours	Credit Factor
0612554 05A	SEC/CU/CS/CR/05/5/MA	Install and Configure Linux	150	15
0612554 06A	SEC/CU/CS/CR/06/5/MA	Secure Software Application	150	15
0413 441 03A	SEC/CU/CS/BC/03/5/MA	Entrepreneurial Skills	40	4
Total hours			**340**	**34**

INSTALL AND CONFIGURE LINUX

ISCED UNIT CODE: 0612554 05A

TVET CDACC UNIT CODE: SEC/CU/CS/CR/05/5/MA

Relationship to Occupational Standards

This unit addresses the core competency required to**:** Install and Configure Linux operating system

Duration of Unit: 150 hours

Unit description

This unit covers the competencies required for installing, configuring, and administering a Linux operating system. It entails mastering the Linux command line, managing file systems and storage, and handling software package management. Additionally, it includes managing system services, users, and groups to ensure efficient system operation. Trainees will also gain expertise in network management, configuring critical server roles, and implementing security measures to safeguard the Linux operating while reinforcing best practices in system administration.

Summary of Learning Outcomes

Learning Outcomes	Durations (Hours)
1. Install and configure Linux Operating system	20
2. Execute Linux Commands in the terminal	30
3. Manage File systems and storage	20
4. Administer users and Groups	10
5. Manage system services and software packages	20
6. Configure Network settings and Server Roles	20
7. Implement Linux Security Measures	20
8. Apply Best Practices in Linux System Administration	10
Total Hours	**150**

Learning Outcomes, Content and Methods of Assessment

Learning Outcome	Content	Methods of Assessment
1. Install and configure a Linux Operating System	1.1 Linux Distributions: 1.1.1 Ubuntu 1.1.2 CentOS 1.1.3 Debian 1.1.4 Other Distros 1.2 Installing Linux on VMware, VirtualBox, and/or Bare Metal 1.3 Partitioning disks. 1.4 Setting up users, system updates, and basic customization 1.5 Troubleshooting installation issues.	• Practical • Observation • Oral • Written
2.1 Execute Linux commands in the terminal.	2.1 Understanding the Linux Shell 2.1.1 Basic syntax and command structure 2.2 File and Directory Management 2.2.1 Navigating the file system 2.2.2 Creating, moving, copying, and deleting files 2.3 User and Permission Management 2.3.1 Understanding user roles and groups 2.3.2Managing file permissions 2.4 Process and System Monitoring 2.4.1 Checking running processes 2.4.2 Monitoring system resources 2.5 Package Management 2.5.1 Installing and updating software 2.5.2 Searching and removing packages 2.6 Networking Commands 2.6.1 Checking connectivity 2.6.2 Viewing network configuration	• Practical • Observation • Written • Oral

	2.7 Redirection and Piping 2.7.1 Combining commands with pipes 2.7.2 Redirecting input and output	
3. Manage File Systems and Storage	3.1 Understanding Linux file system hierarchy 3.1.1 Key directories and their functions 3.2 Disk partitioning and formatting 3.2.1 Fdisk Commands 3.2.2 Mkfs commands 3.2.3 Lsblk commands 3.3 Mounting and unmounting file systems 3.3.1 Manual and Persistent Mounts 3.4 Logical volume manager (LVM) 3.4.1 Creating and managing logical volumes 3.4.2 RAID Configuration	• Written • Oral • Observation • Practical
4. Administer Users and Groups	4.1 Administer users and groups 4.1.1 User Management 4.1.2 Creating, Modifying, and Deleting Users 4.2 Group Management 4.2.1 Assigning Users to Groups and Setting Group Permissions 4.3 User Authentication 4.3.1 Configuring SSH Key-Based Authentication 4.4 Password policies. 4.4.1 Enforcing strong passwords and expiry policies	• Written • Oral • Observation • Practical

	4.5 Restricting access 4.5.1 Using Pseudo and /etc sudoers for privileged access	
5. Manage System Services and Software Packages	5.1 Service Management 5.1.1 Starting, stopping, enabling, and disabling services. 5.2 Package Management 5.2.1 Using APT, YUM, and DNF to Install and update software 5.3 Compiling software from source 5.3.1 Understanding GCC (GNU Compiler collection 5.4 Automating updates 5.4.1 Setting up unattended upgrades in Linux 5.5 Monitoring Services 5.5.1 Checking logs and diagnosing failures	• Written • Oral • Observation • Practical
6. Configure Network Settings and Server Roles	6.1 Configuring IP Addresses and DNS 6.1.1 Using netplan, nmcli, and resolv.conf 6.2 Setting Up a Linux DHCP and DNS Server 6.3 Webserver configuration 6.3.1 Setting up Apache and Nginx with virtual host 6.4 Firewall and port management 6.4.1 Using Iptables,UFW and firewalld 6.5 SSH Configuration 6.5.1 Hardening and Managing Remote Access	• Written • Oral • Observation • Practical

7. Implement Linux Security Measures	7.1 Firewall Rules 7.1.1 Configuring iptables, UFW and SElinux/AppArmor 7.2 Intrusion Detection and Prevention 7.2.1 Installing and Configuring Fail2Ban and Snort 7.3 File integrity monitoring Using AIDE and Auditd for security logging 7.4 System Hardening 7.4.1 Disabling Unused Services, Enforcing Strong SSH Policies 7.5 Security Updates and Patch Management 7.4.1 Keeping Linux Secure with Automatic Updates	• Written • Oral • Observation • Practical
8 Apply Best Practices in Linux System Administration	8.1 Backup and Recovery Strategies 8.1.1 Using rsync, tar, and cron for Automated Backups 8.1.2 Log Management and Monitoring 8.1.3 Using journalctl, syslog, and logrotate 8.2 Performance tuning 8.3 Optimising system performance with Sysctl and top 8.4 Disaster Recovery Planning 8.4.1 Preparing for System Failures and Restoring from Backups 8.5 Documentation and Compliance 8.5.1 Maintaining Proper Documentation and Meeting Security Standards	• Written • Oral • Observation • Practical

Suggested Methods of Instruction

- In Instructor led facilitation of theory
- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos
- Group discussions

Recommended Resources for 25 trainees

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			
1.	Textbooks		13 pcs	13:1
2.	Installation manuals		5pcs	5:1
3.	Charts			
4.	PowerPoint presentations	For trainer's use		
B	**Learning Facilities & infrastructure**			
5.	Lecture/theory room		1	25:1
6.	Computer Laboratory		1	25:1
7.	Internet Connection			
C	**Consumable materials**			
8.	Printing papers		1 ream	1:20
9.	Toners		2 pcs	13:1
10.	Assorted colour of whiteboard markers			
D	**Tools and Equipment**			
11.	Computers/smartphones		25 pcs	1:1
12.	Projector		1 pc	25:1
13.	VMware/Oracle virtual box		25 pc	1:1
14.	Linux distribution		25 pc	1:1

SECURE SOFTWARE APPLICATION

ISCED UNIT CODE: 0612554 06A

TVET CDACC UNIT CODE: SEC/CU/CS/CR/06/5/MA

Relationship to Occupational Standards

This unit addresses the unit of competency: Secure Software Application

Duration of Unit: 150 hours

Unit Description

This unit covers the competencies required to secure software application. It involves identifying software to be secured, establishing tools for application security assessment, perform application security assessment, hardening software application, monitoring application security performance and preparing of reports on software security.

Summary of Learning Outcomes

Learning Outcomes	Durations (Hours)
1. Identify software to be secured	20
2. Establish tools for application security assessment	20
3. Perform application security assessment	30
4. Harden software application	30
5. Monitor application security performance	30
6. Prepare a report on software security	20
Total Hours	**150**

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Identify software to be secured	1.1 Meaning of Terms 1.2 Types of software 1.3 Classification of software and their application 1.4 Factors influencing software selection 1.5 Identify Software That Needs Security 1.6 Identify existing list of installed software 1.7 Check software security updates 1.8 Research CVE Vulnerabilities for listed software	• Observation • Written tests • Oral questioning • Practical tests
2. Establish tools for application security assessment	2.1 Types of tools used in software application security assessment 2.2 Assessing software application 2.2.1 Input Validation 2.2.2 Session Management 2.2.3 Error Handling 2.3 OWASP Security Knowledge framework (SKF) Threat Modelling 2.4 Perform common vulnerabilities. 2.5 Asses the security posture of a web application 2.6 Conduct security assessment using tools	• Observation • Written tests • Oral questioning • Practical tests
3. Perform application security assessment	3.1 Introduction to application security 3.2 Phases of application security assessment 3.3 Reconnaissance and information	• Observation • Written tests • Oral questioning • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	gathering 3.3.1 Passive information gathering 3.3.2 Active information gathering 3.4 Threat modelling 3.4.1 STRIDE model 3.4.2 PASTA model 3.5 Vulnerability Assessment 3.5.1 Manual Testing 3.5.2 Automated Scanning Tools 3.6 Exploitation and verification 3.7 Best Practices	
4. Harden software application	4.1 Introduction to Software Hardening 4.2 Basic security principles for software applications. 4.3 Software configuration 4.4 Common threats to applications. 4.5 Software Vulnerabilities 4.5.1 Injection Attacks (SQL Injection, Command Injection). 4.5.2 Broken Authentication and Session Management. 4.5.3 Cross-Site Scripting (XSS). 4.5.4 Insecure Deserialization. 4.5.5 Misconfigured Security Headers. 4.6 Security measures in software application 4.7 Hardening techniques 4.7.1 Secure coding practices 4.7.2 Applying least privilege principle 4.7.3 Secure configuration of software	• Observation • Written tests • Oral questioning • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	components 4.7.4 Secure deployment and monitoring	
5. Monitor application security performance	5.1 Factors to consider in monitoring of application security performance 5.2 Implementation of monitoring solutions 5.3 Logs management and monitoring 5.4 Key Metrics to Monitor 5.4.1 Failed Login Attempts 5.4.2 Unusual API Requests 5.4.3 Changes in Application Files 5.5 Web applications logs and log management tools 5.5.1 Apache/Nginx logs -Access error and Security logs for web server Monitoring 5.5.2 IIS logs 5.5.3 ELK Stark 5.6 Advanced monitoring tools and techniques. 5.6.1 Security Information and Even Management (SIEM) tools 5.6.2 Web application firewall (WAF) and security monitoring. 5.6.3 Threat hunting with AI and Machine learning	• Observation • Written tests • Oral questioning • Practical tests
6. Prepare a report on software security	6.1 Application summary 6.1.1 Overview of the application 6.1.2 Security goals	• Observation • Written tests • Oral questioning

Learning Outcome	Content	Suggested Assessment Methods
	6.1.3 Key findings 6.2 Methodology 6.2.1 Assessment approach 6.2.2 Tools used 6.2.3 Testing environment 6.3 Vulnerabilities and Risks 6.3.1 Identified vulnerabilities 6.3.2 Severity and impact 6.3.3 Risk rating methodology 6.4 Security Controls 6.4.1 Existing security measures 6.4.2 Effectiveness 6.5 Recommendations 6.5.1 Security improvements 6.5.2 Best practices 6.5.3 Remediation timeline 6.6 Conclusion 6.7 Appendices 6.7.1 Detailed findings 6.7.2 References	• Practical tests

Suggested Methods of Instructions

- In Instructor led facilitation of theory
- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos
- Group discussions

Recommended Resources for 25 trainees.

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			
1.	Textbooks		13 pcs	13:1
2.	Installation manuals		5pcs	5:1
3.	Charts			
4.	PowerPoint presentations	For trainer's use		
B	**Learning Facilities & infrastructure**			
5.	Lecture/theory room		1	25:1
6.	Computer Laboratory		1	25:1
7.	Internet Connection			
C	**Consumable materials**			
8.	Printing papers		1 ream	1:20
9.	Toners		2 pcs	13:1
10.	Assorted colour of whiteboard markers			
D	**Tools and Equipment**			
11.	Computers/Smartphones		25 pcs	1:1
12.	Projector		1 pc	25:1
13.	VMware/Oracle virtual box		25 pc	1:1
14.	Kali Linux or Parrot OS		25 pc	1:1

ENTREPRENEURIAL SKILLS

ISCED UNIT CODE: 0413 441 03A

TVET CDACC UNIT CODE: SEC/CU/CS/BC/03/5/MA

Duration of unit: 40 hours

Relationship to occupational standards

This unit addresses the unit of competency: Apply Entrepreneurial skills.

Unit Description:

This unit covers the competencies required to demonstrate an understanding of entrepreneurship. It involves the ability to: apply financial literacy, apply entrepreneurial concepts, identify entrepreneurship opportunities, apply business legal aspects, innovate business strategies, and develop business plans.

Summary of Learning Outcomes

LEARNING OUTCOMES	DURATION (HOURS)
1. Apply financial literacy	5
2. Apply the entrepreneurial concept	5
3. Identify entrepreneurship opportunities	5
4. Apply business legal aspects	10
5. Innovate Business Strategies	5
6. Develop business plan	10
TOTAL	**40**

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Apply financial literacy	1.1 Personal finance management 1.2 Balancing between needs and wants 1.3 Budget Preparation	• Observation • Project • Written assessment

	1.4 Savings management 1.5 Factors to consider when deciding where to save 1.6 Debt management 1.7 Factors to consider before taking a loan 1.8 Investment decisions 1.9 Types of investments 1.10 Factors to consider when investing money 1.11 Insurance services 1.11.1 Insurance products available in the market 1.11.2 Insurable risks	• Oral assessment • Third party report • Interviews
2. Apply entrepreneurial concept	2.1 Difference between Entrepreneurs and Business persons 2.2 Types of entrepreneurs 2.3 Ways of becoming an entrepreneur 2.4 Characteristics of Entrepreneurs 2.5 Salaried employment and self-employment 2.6 Requirements for entry into self-employment 2.7 Roles of an Entrepreneur in an enterprise 2.8 Contributions of Entrepreneurship	• Observation • Project • Written assessment • Oral assessment • Third party report
3 Identify entrepreneurship opportunities	3.1 Sources of business ideas 3.2 Factors to consider when evaluating business opportunity	

	3.3 Business life cycle	
4 Apply business legal aspects	4.1 Forms of business ownership 4.2 Business registration and licensing processing 4.3 Types of contracts and agreements 4.4 Employment laws 4.5 Taxation laws	• Observation • Written assessment • Project • Oral assessment • Third party report
5 Innovate business Strategies	5.1 Creativity in business 5.2 Innovative business strategies 5.3 Entrepreneurial Linkages 5.4 ICT in business growth and development	• Observation • Written assessment • Project • Oral assessment • Third party report
6 Develop Business Plan	6.1 Business description 6.2 Marketing plan 6.3 Organizational/Management plan 6.4 Production/operation plan 6.5 Financial plan 6.6 Executive summary 6.7 Business plan presentation 6.8 Business idea incubation	• Observation • Written assessment • Project • Oral assessment Third party report

Suggested Methods of Instruction

- Direct instruction with active learning strategies
- Project (Business plan)
- Case studies
- Field trips
- Group Discussions
- Demonstration
- Question and answer
- Problem solving
- Experiential

- Team training
- Guest speakers

Recommended Resources for 25 Trainees

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			
1.	Textbooks		5 pcs	5:1
2.	Business plan templates		5 pcs	5:1
3.	Business Journals		5 pcs	5:1
4.	Newspapers and Handouts			
5.	PowerPoint presentations	For trainer's use		
6.	Assorted colour of whiteboard markers	For trainer's use	2 packets	
7.	e-Didactics	For trainer's use		
8.	Flashcards			
9.	Flip charts			
10.	Whiteboard			
B	**Learning Facilities & infrastructure**			
11.	Lecture/theory room		1	25:1
C	**Consumable materials**			
12.	Printing Papers		1 ream	1:20
13.	Toners		2 pcs	13:1
14.	Internet connection			
D	**Tools and Equipment**			
15.	Projectors		1	25:1
16.	Printers		4	6:1
17.	Computers/Smartphones		25 pcs	1:1

MODULE IV

ISCED Unit Code	TVE CDACC Unit Code	Unit of Learning Title	Duration in Hours	Credit Factor
0612554 07A	SEC/CU/CS/CR/07/5/MA	Perform Website Design and Development	200	20
0612554 08A	SEC/CU/CS/CR/08/5/MA	Conduct Security Assessment and Testing,	150	15
0612554 09A	SEC/CU/CS/CU/01/5/MA	Demonstrate understanding of Cybersecurity Laws, Policies and Regulations	120	12
Total hours			**470**	**47**

PERFORM WEBSITE DESIGN AND DEVELOPMENT

ISCED UNIT CODE: 0612554 07A

TVET CDACC UNIT CODE: SEC/CU/CS/CR/07/5/MA

Relationship to Occupational Standards

This unit addresses the unit of competency: Perform website design and development**.**

Duration of Unit:200hours

Unit Description

This unit specifies competencies required Design a website. It involves gathering data required, determining website design tool, developing functional website, host website developed and perform website routine maintenance.

Summary of Learning Outcomes

Learning Outcomes	Durations (Hours)
1. Gather Data required	20
2. Determine website design tools	30
3. Develop functional website	80
4. Host Website developed	40
5. Monitor Perform Website Routine Maintenance	30
Total Hours	**200**

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Method
1. Gather data required for web site development	1.1 Meaning of web terms. 1.2 Importance of website 1.3 Types of websites 1.4 Website requirements 1.5 Web Programming languages	• Observation • Written • Oral

2. Determine Website design tool	2.2 Types of website authoring tools 2.3 Criteria of choosing website authoring tools 2.4 Installation and configuration of website authoring tools 2.5 Use of website authoring tools	• Observation • Written • Oral
3. Develop functional website	3.1.HTML CODING 3.1.1 Formatting tags 3.1.2 Hyperlinks tag 3.1.3 Tables tags 3.1.4 Frames tags 3.1.5 Forms tags 3.1.6 List tags 3.2.SCRIPTING Functions of scripting languages Types of scripting languages 3.3.Java scripting 3.1.1 JS Statements 3.1.2 JS Variables 3.1.3 JS Operators 3.1.4 JS Data Types 3.1.5 JS Functions 3.1.6 JS Objects 3.1.7 JS Events 3.1.8 JS Strings 3.1.9 JS Numbers 3.1.10 JS Arrays 3.4.PHP 3.4.1 Importance of PHP 3.4.2 PHP Syntax 3.4.3 PHP Variables 3.4.4 PHP Data Types 3.4.5 PHP Operators	• Observation • Written • Oral

	3.4.6 PHP control structures 3.4.7 PHP Functions 3.4.8 PHP Arrays 3.4.9 PHP Forms 3.5. Database Creation 3.6. Database Linkage	
4. Host Website developed	4.1. Website hosting process 4.2. Factors to consider when selecting a host. 4.3. Legal and regulatory requirements 4.4. Domain name 4.5. Uploading web site 4.6. Security measures	• Observation • Written • Oral
5. Perform Website Routine Maintenance	5.1. Importance of website testing 5.2. Components of the website functionalities 5.3. Creation, update and archiving of contents 5.4. Generate maintenance report as per internal policy	• Observation • Written • Oral

Suggested Methods of Delivery

- In Instructor led facilitation of theory
- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos
- Group discussions

Recommended Resources for 25 trainees.

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			
1.	Textbooks		13 pcs	13:1
2.	Installation manuals		5pcs	5:1
3.	Charts			
4.	PowerPoint presentations	For trainer's use		
B	**Learning Facilities & infrastructure**			
5.	Lecture/theory room		1	25:1
6.	Computer Laboratory		1	25:1
7.	Internet Connection			
C	**Consumable materials**			
8.	Printing papers		1 ream	1:20
9.	Toners		2 pcs	13:1
10.	Assorted colour of whiteboard markers			
D	**Tools and Equipment**			
11.	Computers/Smartphones		25 pcs	1:1
12.	Projector		1 pc	25:1
13.	HTML		25 pc	1:1
14.	CMS {Wordpress or Joomla or Drupal}		25 pc	1:1
15.	PHP		25 pc	1:1
16.	Web hosting tools - Xampp		25 pc	1:1

CONDUCT SECURITY ASSESSMENT AND TESTING

ISCED UNIT CODE: 0612554 08A

TVET CDACC UNIT CODE: SEC/CU/CS/CR/08/5/MA

Relationship to Occupational Standards

This unit addresses the unit of competency: Conduct Security Assessment and Testing.

Duration of Unit: 150 hours

Unit Description

This unit covers the competencies required to conduct cyber security assessment and testing. It involves gathering information about organization and its systems, scan and mapping of network, enumerating network resources, exploiting known vulnerabilities, performing social engineering and preparing security assessment and testing report.

Summary of Learning Outcomes

Learning Outcomes	Durations (Hours)
1. Gather Information About Organization and its Systems	20
2. Scan and Map the Network	20
3. Enumerate Target Resources	20
4. Exploit Known Vulnerabilities	30
5. Perform Social Engineering	10
6. Conduct System hacking	40
7. Prepare Security Assessment and Testing Report	10
Total Hours	**150**

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Gather information about organization and its systems	1.1 Explain the importance of reconnaissance on a target system, network, or organization 1.2 Identify different types of reconnaissance: 1.2.1 Active 1.2.2 Passive. 1.3 Use OSINT (Open-Source Intelligence) tools to collect publicly available data. 1.4 Demonstrate the use of WHOIS lookup, DNS enumeration, and Google Dorking. 1.5 Utilise tools like Maltego, theHarvester, and Shodan for information gathering 1.6 Analyse email header and metadata for intelligence gathering	• Observation • Written tests • Oral questioning • Practical tests
2. Scan and map the network	2.1 Understand the purpose of network scanning for security, troubleshooting, and optimization. 2.2 Differentiate between various types of scans 2.2.1 ping scan 2.2.2 SYN scan 2.2.3 TCP scan 2.2.4 UDP scan 2.3 Use Nmap to discover live hosts, open ports, and services.	• Observation • Written tests • Oral questioning • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	2.4 Perform vulnerability scans 2.4.1 Nessus 2.4.2 OpenVAS 2.5 Interpret scan results to identify potential security gaps.	
3. Enumerate target resources	3.1 Enumerate Target Resources 3.2 Define enumeration and its role in cybersecurity and networking. 3.3 Conduct enumeration 3.3.1 File transfer enumeration 3.3.2 DNS enumeration 3.3.3 SMTP enumeration 3.3.4 Website enumeration 3.3.5 Remote connection enumeration 3.4 Perform LDAP and NetBIOS enumeration for directory services 3.5 Identify misconfigurations that could lead to privilege escalation	• Observation • Oral questioning • Practical tests • Written tests
4. Exploit known vulnerabilities	4.1 Use Metasploit Framework to exploit system vulnerabilities. 4.2 Demonstrate privilege escalation techniques on Windows and Linux based systems 4.3 Perform buffer overflow attacks and analyse the results. 4.4 Execute web-based attacks 4.4.1 SQL Injections 4.4.2 XSS 4.4.3 CSRF	• Observation • Written tests • Oral questioning • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
5. Perform social engineering	5.1 Define social engineering. 5.2 Identify different types of social engineering attacks 5.3 Analyse case studies of real-world social engineering attacks. 5.4 Conduct SET (Social-Engineer Toolkit) 5.4.1 Craft phishing emails. 5.5 Develop security awareness strategies to counter social engineering threats. 5.6 Understand ethical configurations and legal aspects of social engineering test	• Observation • Written tests • Oral questioning • Practical tests
6. Conduct System hacking	6.1 Explain the concept and objectives of system hacking in cybersecurity and IT system management 6.2 Demonstrate operating system exploitation techniques 6.2.1 privilege escalation 6.2.2 buffer overflow 6.2.3 kernel vulnerabilities. 6.3 Utilise password cracking tools 6.3.1 brute force 6.3.2 dictionary 6.3.3 rainbow table attacks. 6.4 Analyse hacking tools and frameworks to assess system vulnerabilities. 6.4.1 Metasploit	•

Learning Outcome	Content	Suggested Assessment Methods
	6.5 Deploy keylogging and spyware techniques to capture user credentials and monitor system activity. 6.6 Execute pivoting techniques to move laterally within a compromised network and escalate access privileges. 6.7 Apply methods for covering tracks 6.7.1 log manipulation 6.7.2 anti-forensics techniques 6.7.3 rootkits. 6.8 Implement system hacking countermeasures to mitigate threats. 6.8.1 intrusion detection 6.8.2 endpoint protection 6.9 patch management	
7. Prepare security assessment and testing report	7.1 Explain the significance of assessment and testing reports. 7.2 Document vulnerabilities and their impact based on CVSS scores. 7.3 Structure a professional security assessment report with findings and recommendations. 7.4 Utilise automated reporting tools in assessment and testing. 7.5 Develop remediation strategies based on industry best practice 7.5.1 OWASP 7.5.2 NIST	• Observation • Written tests • Oral questioning • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	7.5.3 ISO 27001 7.6 Present security findings to technical and non-technical stakeholders.	

Suggested Methods of Instruction

- Instructor led facilitation of theory
- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos
- Group discussions

Recommended Resources

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			
1.	Textbooks		13 pcs	13:1
2.	Installation manuals		5pcs	5:1
3.	Charts			
4.	PowerPoint presentations	For trainer's use		
B	**Learning Facilities & infrastructure**			
5.	Lecture/theory room		1	25:1
6.	Computer Laboratory		1	25:1
7.	Internet Connection			
C	**Consumable materials**			
8.	Printing papers		1 ream	1:20
9.	Toners		2 pcs	13:1
10.	Assorted colour of whiteboard			

	markers			
D	**Tools and Equipment**			
11.	Computers/Smartphones		25 pcs	1:1
12.	Projector		1 pc	25:1
13.	VMware/Oracle virtual box		25 pc	1:1
14.	Kali Linux or Parrot OS		25 pc	1:1
15.	Windows 11		25 pc	1:1

DEMONSTRATE UNDERSTANDING OF SECURITY LAWS, POLICIES AND REGULATIONS

ISCED UNIT CODE: 0612554 09A

TVET CDACC UNIT CODE: SEC/CU/CS/CU/01/5/MA

Relationship to Occupational Standards

This unit addresses the unit of competency: Demonstrate understanding of security laws, policies and regulations.

Duration of Unit: 120 hours

Unit Description

This unit covers the competencies required in applying Cyber security laws, policies and regulations. It involves demonstrating the understanding of different cyber security policies and regulations, developing cyber security policy, implementing Cyber security policies and regulations, evaluating Cyber security policies, evaluating compliance in Cyber security policies and regulations and monitoring effectiveness of Cyber security policy in an organization.

Summary of Learning Outcomes

Learning Outcomes	Durations (Hours)
1. Demonstrate understanding of cyber security laws, policies and regulations	20
2. Develop Cyber Security policy	10
3. Implement Cyber Security policy and regulations	30
4. Evaluate Cyber security policy	20
5. Evaluate compliance in Cyber security policy and regulations	10
6. Monitor effectiveness of Cyber security policy in an organization	20
7. Monitor effectiveness of Cyber security	10
Total Hours	**120**

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Demonstrate understanding of cyber security laws	1.1 Meaning of terms 1.1.1 World legal system 1.1.1.1 Common law 1.1.1.2 Religious law 1.1.1.3 Hindu law 1.1.1.4 Islamic law 1.2 Types of Cyber security laws 1.2.1 National 1.2.2 International 1.3 Cyber crimes 1.3.1 Types of cyber crimes 1.3.2 Challenges in prosecuting cyber crime 1.4 Cyber-crime laws 1.4.1 Local Cybercrime laws 1.4.2 International Cybercrime laws 1.5 Application of cyber security laws 1.6 Compliance of cyber security laws 1.7 Impacts of cyber crime 1.7.1 Positive and Negative	• Observation • Oral questioning • Written tests • Practical tests
2. Demonstrate understanding of different Cyber security policies and regulations	2.1 Meaning of terms 2.2 Fundamentals of cyber security 2.3 Types of cyber security policies and regulation 2.4 Application of different cyber security policies 2.5 Stakeholders involved in cyber security policies and regulations 2.6 Regulatory board in cyber security	• Observation • Oral questioning • Written tests • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	policies	
3. Develop Cyber Security policy	3.1 Meaning of terms 3.2 Components of cyber security and information classification 3.3 Cyber security policy alignments to the vision and mission 3.4 Procedures of drafting cyber security policy 3.5 Cyber security review process	• Observation • Oral questioning • Written tests • Practical tests
4. Implement Cyber Security policy and regulations	4.1 Meaning of terms 4.2 Cyber security policy implementation process 4.3 Cyber security policy implementation team 4.4 Importance of schedule in the implementation process of cyber security policy 4.5 Verification of cyber security implementation 4.6 Relevant regulations in implementation of cyber security policy	• Observation • Oral questioning • Written tests • Practical tests
5. Evaluate Cyber security policy	5.1 Meaning of terms 5.2 Review and updates of cyber security policy 5.3 Process of evaluation of cyber security policy 5.4 Factors to consider in evaluation of cyber security policy	• Observation • Oral questioning • Written tests • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
6. Evaluate compliance in Cyber security policy and regulations	6.1 Meaning of terms 6.2 Infrastructure and landscape audit 6.3 Calculation of risk factors 6.4 Calculation of non – compliance factors 6.5 Compliance level recommendation	• Observation • Oral questioning • Written tests • Practical tests
7. Monitor effectiveness of Cyber security policy in an organization	7.1 Meaning of terms 7.2 Compliance level 7.3 Cyber security policy monitoring impact on: 7.3.1 Process 7.3.2 People 7.3.3 Technology 7.4 Monitoring effectiveness of cyber security policy	• Observation • Oral questioning • Written tests • Practical tests

Suggested Delivery Methods

- In Instructor led facilitation of theory
- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos
- Group discussions
- Case study.

Recommended resources for 25 trainees

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			
1.	Textbooks		13 pcs	13:1
2.	Installation manuals		5pcs	5:1
3.	Charts			

4.	PowerPoint presentations	For trainer's use		
B	**Learning Facilities & infrastructure**			
5.	Lecture/theory room		1	25:1
6.	Computer Laboratory		1	25:1
7.	Internet Connection			
C	**Consumable materials**			
8	Printing papers		1 ream	1:20
9.	Toners		2 pcs	13:1
10.	Assorted colour of whiteboard markers			
D	**Tools and Equipment**			
11.	Computers		25 pcs	1:1
12.	Projector		1 pc	25:1

MODULE V

ISCED Unit Code	TVE CDACC Unit Code	Unit of Learning Title	Duration in Hours	Credit Factor
0612554 09A	SEC/CU/CS/CR/01/6/MA	Build Secure Networks	120	12
0612554 10A	SEC/CU/CS/CR/02/6/MA	Manage Security Operations	160	16
0612554 11A	SEC/CU/CS/CR/03/6/MA	Develop Computer Software	200	20
Total hours			**480**	**48**

BUILD SECURE NETWORK

ISCED UNIT CODE: 0612554 10A

TVET CDACC UNIT CODE: SEC/CU/CS/CR/01/6/MA

Relationship to Occupational Standards

This unit addresses the unit of competency: Build secure network

Duration of Unit: 120 hours

Unit Description

This unit covers the competencies required in building secure network. It involves reviewing security issues, analyzing network security protocols and features, designing and perimeters, installing and configuring perimeter solutions, configuring internal network devices, testing and verifying design performance and training network users.

Summary of Learning Outcomes

Learning Outcomes	Durations (Hours)
1. Review security issues	30
2. Analyze network security protocols and features	20
3. Install and configure perimeter solutions	40
4. Test and verify design performance	20
5. Train network users	10
Total Hours	**120**

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Review security issues	1.1 Importance of Network Security 1.2 Common Threats and Attacks 1.3 Security Monitoring and Analysis Tools: 1.3.1 Wireshark (Packet Analysis) 1.4 Hardening Network Devices 1.5 Secure Remote Management	• Observation • Oral questioning • Written tests • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	1.6 Configure Access Control Lists (ACLs)	
2. Analyse network security protocols and features	2.1 Encryption and Secure Communication Protocols 2.1.1 SSL/TLS (Secure Sockets Layer/ Transport Layer Security) 2.1.2 IPsec (Internet Protocol Security) 2.1.3 WPA2/WPA3 (Wi-Fi Protected Access) 2.2 Secure Data Transfer Protocols 2.2.1 HTTPS (Hypertext Transfer Protocol Secure) 2.2.2 SFTP (Secure File Transfer Protocol) 2.2.3 FTPS (File Transfer Protocol Secure) 2.3 Network Device Security Protocols 2.3.1 SSH (Secure Shell) 2.3.2 SNMPv3 (Simple Network Management Protocol v3)	• Observation • Oral questioning • Written tests • Practical tests
3. Install and configure perimeter solutions	3.1 Meaning of Terms 3.2 Factors to consider in acquiring perimeter solutions 3.3 Factors to consider in installation of perimeter solution 3.4 Configure Firewalls 3.4.1 Physically connect the firewall between two networks 3.5 Configure Intrusion Detection and Prevention Systems (IDS/IPS) 3.5.1 Configure IDS/IPS rules 3.5.2 Set up alerts to notify admins about suspicious activity.	• Observation • Oral questioning • Written tests • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	3.6 Configure Virtual Private Network (VPN) 3.6.1 Create VPN user accounts with strong passwords. 3.6.2 Enable multi-factor authentication (MFA). 3.6.3 Use AES-256 encryption for strong security.	
4. Test and verify design performance	4.1 Define testing objectives 4.2 Create a test plan 4.3 Conduct network performance testing 4.4 Conduct network security testing 4.5 Conduct redundancy testing.	• Observation • Oral questioning • Written tests • Practical tests
5. Train network users	5.1 Identify training objectives 5.2 Tailor security training to user roles 5.3 Network usage best practices	• Written tests • Oral questioning • Practical tests • Observation

Suggested Delivery Methods

- In Instructor led facilitation of theory
- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos
- Group discussions

Recommended resources for 25 trainees

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			
1.	Textbooks		13 pcs	13:1
2.	Installation manuals		5pcs	5:1
3.	Charts			

4.	PowerPoint presentations	For trainer's use		
B	**Learning Facilities & infrastructure**			
5.	Lecture/theory room		1	25:1
6.	Computer Laboratory		1	25:1
7.	Internet Connection			
C	Consumable materials			
8.	Printing papers		1 ream	1:20
9.	Toners		2 pcs	13:1
10.	Assorted colour of whiteboard markers			
D	**Tools and Equipment**			
11.	Computers		25 pcs	1:1
12.	Projector		1 pc	25:1
13.	Signal testers		5 pcs	5:1
14.	Header checker		25 pcs	1:1
15.	Crimping tools		25 pcs	1:1
16.	Cable tester		5 pcs	5:1
17.	Switches		5pcs	5:1
18.	Repeaters		5pcs	5:1
19.	Routers/modem		5pcs	5:1
20.	Network tool kit		25 pcs	1:1
21.	RJ45		300 pcs	1:10
22.	UTP Ethernet Cable		300 mtrs	1:10
23.	Antistatic gloves		25 pairs	1:1
24.	Wireshark 32/64-bit Latest version		25 pc	1:1
25.	Network simulation tools: -Cisco packet tracer or -GNS3		25 pc	1:1
26.	VMware/Oracle virtual box		25 pc	1:1
27.	Kali Linux or Parrot OS		25pc	1:1

MANAGE SECURITY OPERATIONS

ISCED UNIT CODE: 0612554 11A

TVET CDACC UNIT CODE: SEC/CU/CS/CR/02/6/MA

Relationship to Occupational Standards

This unit addresses the unit of competency: Manage security operations

Duration of Unit: 160 hours

Unit Description

This unit covers the competencies required to manage security operations and risks related to cybersecurity. It comprises establishing asset inventory risks, assessing threat risk factors and implementing a security management solution. It entails monitoring security events, updating risk profile, responding to established threats and generating security operation reports.

Summary of Learning Outcomes

Learning Outcomes	Durations (Hours)
1. Establish asset inventory risks	20
2. Assess threat risk factors	20
3. Establish threats landscape	10
4. Implement security management solutions	30
5. Monitor security events	30
6. Update risk profile	20
7. Respond to established threats	20
8. Generate security operations reports	10
Total Hours	**160**

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Establish asset inventory risks	1.1 Identify and classify assets based on business value and criticality. 1.2 Analyse potential vulnerabilities associated with hardware, software, and data. 1.3 Evaluate exposure to environmental, operational, and cyber threats.	• Observation • Oral questioning • Practical tests • Written tests
2. Assess threat risk factors	2.1 Identify potential threat actors, including internal and external sources. 2.2 Analyze likelihood and impact of threats using qualitative and quantitative methods. 2.3 Utilize threat intelligence to enhance risk assessment accuracy.	• Observation • Oral questioning • Practical tests • Written tests
3. Establish threats landscape	3.1 Meaning of terms 3.2 Threats identification and modelling 3.3 Threat mitigation measures	• Observation • Oral questioning • Practical tests • Written tests
4. Implement security management solutions	4.1 Deploy access controls, encryption, and endpoint security measures. 4.2 Apply security policies, standards, and frameworks for risk mitigation. 4.3 Utilize automation tools for threat detection and response.	• Observation • Oral questioning • Practical tests • Written tests

Learning Outcome	Content	Suggested Assessment Methods
5. Monitor security events	5.1 Deploy real-time monitoring tools such as SIEM, IDS/IPS, and endpoint detection. 5.2 Analyze security logs, alerts, and anomalies for potential threats. 5.3 Establish baselines for normal system behaviour to detect deviations. 5.4 Automate correlation of security events to identify attack patterns. 5.5 Continuously assess network traffic and user activity for suspicious behaviour.	• Observation • Oral questioning • Practical tests • Written tests
6. Update risk profile	6.1 Review risk levels based on emerging threats and vulnerabilities. 6.2 Integrate threat intelligence feeds to enhance risk awareness. 6.3 Update asset classification and security controls to align with changing risks. 6.4 Conduct periodic security audits and vulnerability assessments.	• Observation • Oral questioning • Practical tests • Written tests
7. Respond to established threats.	7.1 Initiate incident response plans and containment procedures. 7.2 Conduct forensic investigations to determine root causes. 7.3 Apply remediation measures and update security policies.	• Observation • Oral questioning • Practical tests • Written tests
8. Generate Security Operations Reports	8.1 Document security incidents, trends, and response actions. 8.2 Use dashboards and metrics to communicate security posture	• Observation • Oral questioning • Practical tests • Written tests

Learning Outcome	Content	Suggested Assessment Methods
	effectively. 8.3 Provide compliance reports for regulatory and organizational requirements. 8.4 Communicate risk adjustments to stakeholders.	

Suggested Delivery Methods

- In Instructor led facilitation of theory
- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos
- Group discussions

Recommended resources for 25 trainees

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			
1.	Textbooks		13 pcs	13:1
2.	Installation manuals		5pcs	5:1
3.	Charts			
4.	PowerPoint presentations	For trainer's use		
B	**Learning Facilities & infrastructure**			
5.	Lecture/theory room		1	25:1
6.	Computer Laboratory		1	25:1
7.	Internet Connection			
C	**Consumable materials**			

8	Printing papers		1 ream	1:20
9.	Toners		2 pcs	13:1
10.	Assorted colour of whiteboard markers			
D	**Tools and Equipment**			
11.	Computers		25 pcs	1:1
12.	Projector		1 pc	25:1
13.	Wireshark 32/64-bit Latest version		25 pc	1:1
14.	VMware/Oracle virtual box		25 pc	1:1
15.	Kali Linux or Parrot OS		25pc	1:1

DEVELOP COMPUTER SOFTWARE

ISCED UNIT CODE: 0612554 12A

TVET CDACC UNIT CODE: SEC/CU/CS/CR/03/6/MA

Relationship to Occupational Standards

This unit addresses the unit of competency: Develop computer software

Duration of Unit: 200 hours

Unit Description

This unit covers the competencies required to develop computer software. It involves establishing software purpose, analysing software requirements, designing computer software, developing computer software, performing programme testing and maintenance.

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Identify the fundamentals to programming	1.1 Definition of terms 1.2 History of programming language 1.3 Level of programming languages 1.4 Types of programming languages 1.5 Programming paradigms 1.6 Hardware and Software considerations for object-oriented programming 1.7 Programming Development Life Cycle	• Observation • Oral questioning • Written tests • Practical tests
2. Design computer software	2.1 Program design tools 2.1.1 Pseudocodes 2.1.2 Algorithms 2.1.3 Flowcharts 2.1.4 Data Flow Diagrams	• Observation • Oral questioning • Practical tests • Written tests

Learning Outcome	Content	Suggested Assessment Methods
3. Develop computer software using an object-oriented programming language (JAVA, C++ or PYTHON)	3.1 Language structure 3.2 Features of OOP languages 3.2.1 Program writing using C++ or Python or java. 3.2.2 Basic syntax 3.2.2.1 Comments 3.2.2.2 Keywords 3.2.2.3 Importance of syntax in programming 3.2.2.4 Guidelines for naming conventions and best practices 3.3 Input and output statements 3.4 Variables 3.4.1 Types of variables 3.4.2 Variable declaration 3.4.3 Variable initialization 3.5 Data types 3.6 Operators 3.7 Program Control structures 3.7.1.1 Sequential 3.7.1.2 Selection 3.7.1.3 Switch statements 3.7.1.4 Iteration 3.8 Concepts in OOP 3.8.1 Objects and classes 3.8.2 Inheritance 3.8.3 Polymorphism 3.8.4 Encapsulation 3.8.5 Constructors 3.8.6 Operator overloading 3.9 Functions	• Observation • Oral questioning • Written tests • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	3.10 Methods 3.11 Data structures 3.11.1 Arrays 3.11.2 Pointers 3.11.3 Queues 3.11.4 Stack 3.11.5 Lists 3.11.6 Dictionaries 3.11.7 Tuples 3.12 File extensions in OOP 3.12.1 File stream 3.12.2 Features/properties 3.12.3 File operations 3.12.4 File handling	
4. Perform programme testing	4.1 Types of tests 4.1.1 Software functionality testing 4.1.2 Software security testing 4.2 Software debugging 4.3 Software reporting and testing 4.4 Quality assurance and testing	• Observation • Oral questioning • Written tests • Practical tests
5. Perform software implementation and maintenance	5.1 Meaning of terms 5.2 User acceptance and implementation 5.3 Preparation of software maintenance schedule 5.4 Software patch management 5.5 Software version control 5.6 Software review 5.7 Software monitoring and evaluation	• Observation • Oral questioning • Written tests • Practical tests

Suggested Delivery Methods

- In Instructor led facilitation of theory

- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos
- Group discussions

Recommended resources for 25 trainees

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	**Learning Materials**			
1.	Textbooks		13 pcs	13:1
2.	Installation manuals		5pcs	5:1
3.	Charts			
4.	PowerPoint presentations	For trainer's use		
B	**Learning Facilities & infrastructure**			
5.	Lecture/theory room		1	25:1
6.	Computer Laboratory		1	25:1
7.	Internet Connection			
C	**Consumable materials**			
8	Printing papers		1 ream	1:20
9.	Toners		2 pcs	13:1
10.	Assorted colour of whiteboard markers			
D	**Tools and Equipment**			
11.	Computers		25 pcs	1:1
12.	Projector		1 pc	25:1
15.	Visual Studio Code (VS Code)		25pc	1:1

MODULE VI

INDUSTRY TRAINING	**480**	**48**
Total hours	**480**	**48**

INDUSTRY TRAINING

An individual enrolled in this course will be required to undergo Industry training for a minimum period of 480 hours in Cyber Security Sector upon completion of Module IV. The industrial training may be taken after completion of all units for those pursuing the full qualification or be distributed equally in each unit for those pursuing part qualification. In the case of dual training model, industrial training shall be as guided by the dual training policy