REPUBLIC OF KENYA

COMPETENCY BASED CURRICULUM

FOR

CYBER SECURITY LEVEL 6

TVET CDACC
P.O BOX 15745-00100
NAIROBI

First published 2019

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 economic development. Quality education and training will contribute to achievement Kenya's development blue print and sustainable development goals.

Reforms in the education sector are necessary for the achievement of Kenya Vision 2030 and meeting the provisions of the Constitution of Kenya 2010. The education sector had to be aligned to the Constitution and this resulted to the formulation of the Policy Framework for Reforming Education and Training. A key feature of this policy is the radical change in the design and delivery of the 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 mode of delivery allows 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.

It is my conviction that this curriculum will play a great role towards development of competent human resource for the Security sector's growth and sustainable development.

PRINCIPAL SECRETARY, VOCATIONAL AND TECHNICAL TRAINING

MINISTRY OF EDUCATION

PREFACE

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

The Technical and Vocational Education and Training Act No. 29 of 2013 on Reforming Education and Training in Kenya, 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 Kenyan labour force.

TVET Curriculum Development, Assessment and Certification Council (TVET CDACC), in conjunction with Security Sector Skills Advisory Committee (SSAC) have developed this curriculum.

This curriculum has been developed following the CBET framework policy; the CBETA standards and guidelines provided by the TVET Authority and the Kenya National Qualification Framework designed by the Kenya National Qualification Authority.

This curriculum is designed and organized with an outline of learning outcomes; suggested delivery methods, training/learning resources and methods of assessing the trainee's achievement. The curriculum is competency-based and allows multiple entry and exit to the course.

I am grateful to the Council Members, Council Secretariat, Security SSAC, expert workers and all those who participated in the development of this curriculum.

CHAIRPERSON,

TVET CDACC

ACKNOWLEDGEMENT

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 was received from various organizations.

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

I am convinced that this curriculum will go a long way in ensuring that workers in Security Sector acquire competencies that will enable them to perform their work more efficiently.

COUNCIL SECRETARY/CEO

TVET CDACC

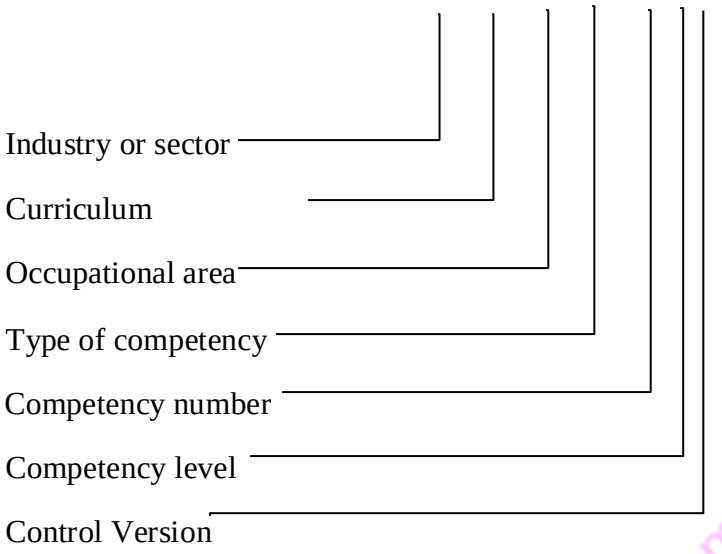
TABLE OF CONTENTS

ACRONYMNS AND ABBREVIATIONS

A	Control Version
BC	Basic Competencies
CC	Common Competencies
CDACC	Curriculum Development, Assessment and Certification Council
CERT	Computer Incidence response team
CIRT	Computer Incidence response team
CS	Cyber Security
CR	Core Competencies
CU	Curriculum
EHS	Environment, Health and Safety
IBMS	Integrated Building Management System
ICT	Information and communication Technology
IEE	Institute of Electrical Engineers
KEBS	Kenya Bureau of Standards
NCA	National Construction Authority
NIST	National institute of Standards and Technology
OSHA	Occupational Safety and Health Act
OWASP	Open web application security Project
PPE	Personal Protective Equipment
SEC	Security
SIEM	Security Information and Event management
TVET	Technical and Vocational Education and Training
WIBA	Work injury benefits Act

KEY TO UNIT CODE

SEC/CU/CS/BC/01/6/A



OVERVIEW

Description of the course

This course is designed to equip a Cyber security technician with the competencies required to perform computer repair and maintenance, apply cyber security laws, policies and regulations, perform computer networking, software application security, database security, cyber security system installation, cyber security risk assessment, security assessment and testing and security operation management.

The course consists of basic, common and core units of learning as indicated below:

Basic Units of Learning

Unit Code	Unit Title	Duration in Hours	Credit Factors
SEC/CU/CS/BC/01/6/A	Communication skills	40	4
SEC/CU/CS/BC/02/6/A	Numeracy skills	60	6
SEC/CU/CS/BC/03/6/A	Entrepreneurial skills	100	10
SEC/CU/CS/BC/04/6/A	Employability skills	80	8
SEC/CU/CS/BC/05/6/A	Environmental literacy	40	4
SEC/CU/CS/BC/06/6/A	Occupational safety and health practices	40	4
Total		**360**	**36**

Common Units of Learning

Unit Code	Unit Title	Duration in Hours	Credit Factors
SEC/CU/CS/CC/01/6/A	Digital Literacy	60	6
Total		**60**	**6**

Core Units of Learning

Unit Code	Unit Title	Duration in Hours	Credit Factors
SEC/CU/CS/CR/01/6/A	Computer repair and maintenance	120	12
SEC/CU/CS/CR/02/6/A	Cyber security laws, policies and regulations	190	19
SEC/CU/CS/CR/03/6/A	Computer Networking	130	13
SEC/CU/CS/CR/04/6/A	Building of secure network	120	12
SEC/CU/CS/CR/05/6/A	Computer software development	130	13
SEC/CU/CS/CR/06/6/A	Software application security	110	11
SEC/CU/CS/CR/07/6/A	Database Security	70	7
SEC/CU/CS/CR/08/6/A	Cyber security system installation	130	13
SEC/CU/CS/CR/09/6/A	Cyber Security risk assessment	120	12
SEC/CU/CS/CR/10/6/A	Security Assessment and testing	110	11
SEC/CU/CS/CR/11/6/A	Security Operations management		
	Industrial Attachment	480	48
Total		**1,710**	**171**
Grand Total		**2,610**	**261**

Entry Requirements

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

a) Kenya Certificate of Secondary Education (K.C.S.E.) with a minimum mean grade of C- (C minus)

Or

b) Level 5 certificate in a related course with **one** year of continuous work experience

Or

c) Equivalent qualifications as determined by Kenya National Qualifications Authority (KNQA)

d)

Trainer qualification

A trainer for this course should have a higher qualification than the level of this course

Assessment

The course will be assessed at two levels: internally and externally. Internal assessment is continuous and is conducted by the trainer who is monitored by an internal accredited verifier while external assessment is the responsibility of TVET/CDACC.

Certification

A candidate will be issued with a Certificate of Competency on demonstration of competence in a unit of competency. To attain the qualification Cyber security technician Level 6, the candidate must demonstrate competence in all the units of competency as given in qualification pack. These certificates will be issued by TVET CDACC in conjunction with training provider.

BASIC UNITS OF LEARNING

COMMUNICATION SKILLS

UNIT CODE: SEC/CU/CS/BC/01/6/A

Relationship to Occupational Standards
This unit addresses the Unit of Competency: Demonstrate Communication Skills

Duration of Unit: 40 hours

Unit Description
This unit covers the competencies required to demonstrate communication skills .It involves, meeting communication needs of clients and colleagues; developing communication strategies, establishing and maintaining communication pathways, conducting interviews, facilitating group discussion and representing the organization.

Summary of Learning Outcomes

1. Meet communication needs of clients and colleagues
2. Develop communication strategies
3. Establish and maintain communication pathways
4. Promote use of communication strategies
5. Conduct interview
6. Facilitate group discussion
7. Represent the organization

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Meet communication needs of clients and colleagues	• Communication process • Modes of communication • Medium of communication • Effective communication • Barriers to communication • Flow of communication • Sources of information • Organizational policies • Organization requirements for written and electronic communication methods • Report writing	• Interview • Written texts

	• Effective questioning techniques (clarifying and probing) • Workplace etiquette • Ethical work practices in handling communication • Active listening • Feedback • Interpretation • Flexibility in communication • Types of communication strategies • Elements of communication strategy	
2. Develop communication strategies	• Dynamics of groups • Styles of group leadership • Openness and flexibility in communication • Communication skills relevant to client groups	• Interview • Written texts
3. Establish and maintain communication pathways	• Types of communication pathways	• Interview • Written texts
4. Promote use of communication strategies	• Application of elements of communication strategies • Effective communication techniques	• Interview • Written texts
5. Conduct interview	• Types of interview • Establishing rapport • Facilitating resolution of issues • Developing action plans	• Interview • Written texts
6. Facilitate group discussion	• Identification of communication needs • Dynamics of groups • Styles of group leadership • Presentation of information • Encouraging group members participation • Evaluating group communication	• Interview • Written texts

	strategies	
7. Represent the organization	• Presentation techniques • Development of a presentation • Multi-media utilization in presentation • Communication skills relevant to client groups	• Interview • Written texts

Suggested Methods of Instruction

- Discussion
- Role playing
- Simulation
- Direct instruction

Recommended Resources

- Desktop computers/laptops
- Internet connection
- Projectors
- Telephone

NUMERACY SKILLS

UNIT CODE: SEC/CU/CS/BC/02/6/A

Relationship to Occupational Standards
This unit addresses the Unit of Competency: Demonstrate Numeracy Skills.

Duration of Unit: 60 hours

Unit Description
This unit describes the competencies required to demonstrate numeracy skills. It involves applying a wide range of mathematical calculations for work; applying ratios, rates and proportions to solve problems; estimating, measuring and calculating measurement for work; using detailed maps to plan travel routes for work; using geometry to draw and construct 2D and 3D shapes for work; collecting, organizing and interpreting statistical data; using routine formula and algebraic expressions for work and using common functions of a scientific calculator.

Summary of Learning Outcomes

1. Apply a wide range of mathematical calculations for work
2. Apply ratios, rates and proportions to solve problems
3. Estimate, measure and calculate measurement for work
4. Use detailed maps to plan travel routes for work
5. Use geometry to draw and construct 2D and 3D shapes for work
6. Collect, organize and interpret statistical data
7. Use routine formula and algebraic expressions for work
8. Use common functions of a scientific calculator

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods

1. Apply a wide range of mathematical calculations for work	• Fundamentals of mathematics
	  • Addition, subtraction, multiplication and division of positive and negative numbers
	  • Algebraic expressions manipulation
	• Forms of fractions, decimals and percentages
	• Expression of numbers as powers and roots
		• Written tests
		• Assignments
		• Supervised exercises

2. Apply ratios, rates and proportions to solve problems	• Rates, ratios and proportions
	  • Meaning
	  • Conversions into percentages
	  • Direct and inverse proportions determination
	  • Performing calculations
	  • Construction of graphs, charts and tables
	  • Recording of information
		• Written tests
		• Assignments
		• Supervised exercises

3. Estimate, measure and calculate measurement for work	• Units of measurements and their symbols • Identification and selection of measuring equipment • Conversion of units of measurement • Perimeters of regular figures • Areas of regular figures • Volumes of regular figures • Carrying out measurements • Recording of information	• Assignments • Supervised exercises • Written tests
4. Use detailed maps to plan travel routes for work	• Identification of features in routine maps and plans • Symbols and keys used in routine maps and plans • Identification and interpretation of orientation of map to North • Demonstrate understanding of direction and location • Apply simple scale to estimate length of objects, or distance to location or object • Give and receive directions using both formal and informal language • Planning of routes • Calculation of distance, speed and time	• Written • Practical test
5. Use geometry to draw and	• Identify two dimensional shapes and routine three dimensional	

construct 2D and 3D shapes for work	shapes in everyday objects and in different orientations • Explain the use and application of shapes • Use formal and informal mathematical language and symbols to describe and compare the features of two dimensional shapes and routine three dimensional shapes • Identify common angles • Estimate common angles in everyday objects • Evaluation of unknown angles • Use formal and informal mathematical language to describe and compare common angles • Symmetry and similarity • Use common geometric instruments to draw two dimensional shapes • Construct routine three dimensional objects from given nets	

6. Collect, organize and interpret statistical data	• Classification of data
	  • Grouped data
	  • Ungrouped data
	• Data collection
	  • Observation
	  • Recording
	• Distinguishing between sampling and census
	• Importance of sampling
	• Errors in sampling
	• Types of sampling and their limitations e.g.
	  • Stratified random
	  • Cluster
		• Assignments
		• Supervised exercises
		• Written tests

	• Judgmental
	• Tabulation of data
	  • Class intervals
	  • Class boundaries
	  • Frequency tables
	  • Cumulative frequency
	• Diagrammatic and graphical presentation of data e.g.
	  • Histograms
	  • Frequency polygons
	  • Bar charts
	  • Pie charts
	  • Cumulative frequency curves
	• Interpretation of data	

7. Use routine formula and algebraic expressions for work	• Solving linear equations
	• Linear graphs
	  • Plotting
	  • Interpretation
	• Applications of linear graphs
	• Curves of first and second degree
	  • Plotting
	  • Interpretation
		• Assignments
		• Supervised exercises
		• Written tests

8. Use common functions of a scientific calculator	• Identify and use keys for common functions on a calculator • Calculate using whole numbers, money and routine decimals and percentages • Calculate with routine fractions and percentages • Apply order of operations to solve multi-step calculations • Interpret display and record result	• • Written • Practical test

Suggested Methods of Instruction

- Group discussions
- Demonstration by trainer
- Practical work by trainee
- Exercises

Recommended Resources

- Calculators
- Rulers, pencils, erasers
- Charts with presentations of data
- Graph books
- Dice

ENTREPRENEURIAL SKILLS

UNIT CODE: SEC/CU/CS/BC/03/6/A

Relationship to Occupational Standards

This unit addresses the Unit of Competency: Demonstrate Entrepreneurial Skills

Duration of unit: 100 hours

Unit Description

This unit covers the competencies required to demonstrate understanding of entrepreneurship. It involves demonstrating understanding of an entrepreneur, entrepreneurship and self-employment. It also involves identifying entrepreneurship opportunities, creating entrepreneurial awareness, applying entrepreneurial motivation and developing business innovative strategies.

Summary of Learning Outcomes

1. Demonstrate understanding of who an entrepreneur
2. Demonstrate knowledge of entrepreneurship and self-employment
3. Identify entrepreneurship opportunities
4. Create entrepreneurial awareness
5. Apply entrepreneurial motivation
6. Develop business innovative strategies
7. Develop Business plan

Learning Outcome	Content	Suggested Assessment Methods
1. Demonstrate knowledge of entrepreneurship and self-employment	• Importance of self-employment • Requirements for entry into self-employment • Role of an Entrepreneur in business • Contributions of Entrepreneurs to National development • Entrepreneurship culture in Kenya • Born or made entrepreneurs	• Individual/group assignments • Projects • Written tests • Oral questions • Third party report

2. Identify entrepreneurship opportunities	• Business ideas and opportunities • Sources of business ideas • Business life cycle • Legal aspects of business • Assessment of product demand • Business environment • Factors to consider when evaluating business environment • Technology in business	• Individual/group assignments • Projects • Written tests • Oral questions • Third party report • Interviews
3. Create entrepreneurial awareness	• Forms of businesses • Sources of business finance • Factors in selecting source of business finance • Governing policies on Small Scale Enterprises (SSEs) • Problems of starting and operating SSEs	• Individual/group assignments • Projects • Written tests • Oral questions • Third party report • Interviews
4. Apply entrepreneurial motivation	• Internal and external motivation • Motivational theories • Self-assessment • Entrepreneurial orientation • Effective communications in entrepreneurship • Principles of communication • Entrepreneurial motivation	• Case studies • Individual/group assignments • Projects • Written tests • Oral questions • Third party report • Interviews

5. Develop business innovative strategies	• Innovation in business • Small business Strategic Plan • Creativity in business development • Linkages with other entrepreneurs • ICT in business growth and development	• Case studies • Individual/group assignments • Projects • Written tests • Oral questions • Third party report • Interviews
6. Develop Business Plan	• Business description • Marketing plan • Organizational/Management • plan • Production/operation plan • Financial plan • Executive summary • Presentation of Business Plan	• Case studies • Individual/group assignments • Projects • Written tests • Oral questions • Third party report • Interviews

Suggested Methods of Instruction

- Direct instruction
- Project
- Case studies
- Field trips
- Discussions
- Demonstration
- Question and answer
- Problem solving
- Experiential
- Team training

Recommended Resources

- Case studies
- Business plan templates
- Computers
- Overhead projectors
- Internet

- Mobile phone
- Video clips
- Films
- Newspapers and Handouts
- Business Journals
- Writing materials

EMPLOYABILITY SKILLS

UNIT CODE: SEC/CU/CS/BC/04/6/A

Relationship to Occupational Standards
This unit addresses the Unit of Competency: Demonstrate Employability Skills

Duration of Unit: 80 hours

Unit Description
This unit covers competencies required to demonstrate employability skills. It involves conducting self-management, demonstrating interpersonal communication, critical safe work habits, leading a workplace team, planning and organizing work, maintaining professional growth and development, demonstrating workplace learning, problem solving skills and managing ethical performance.

Summary of Learning Outcomes

1. Conduct self-management
2. Demonstrate interpersonal communication
3. Demonstrate critical safe work habits
4. Lead a workplace team
5. Plan and organize work
6. Maintain professional growth and development
7. Demonstrate workplace learning
8. Demonstrate problem solving skills
9. Manage ethical performance

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Conduct self-management	• Self-awareness • Formulating personal vision, mission and goals • Strategies for overcoming life challenges • Managing emotions • Emotional intelligence • Assertiveness versus aggressiveness • Expressing personal thoughts, feelings and beliefs	• Written tests • Oral questioning • Interviewing • Portfolio of evidence • Third party report

	• Developing and maintaining high self-esteem • Developing and maintaining positive self-image • Setting performance targets • Monitoring and evaluating performance • Articulating ideas and aspirations • Accountability and responsibility • Good work habits • Self-awareness • Values and beliefs • Self-development • Financial literacy • Healthy lifestyle practices • Adopting safety practices	
2. Demonstrate interpersonal communication	• Meaning of interpersonal communication • Listening skills • Types of audience • Public speaking • Writing skills • Negotiation skills • Reading skills • Meaning of empathy • Understanding customers' needs • Establishing communication networks • Assertiveness • Sharing information	• Written tests • Oral questioning • Interviewing • Portfolio of evidence • Third party report
3. Demonstrate critical safe work habits	• Stress and stress management • Time concept • Punctuality and time consciousness • Leisure • Integrating personal objectives into organizational objectives • Resources mobilization	• Written tests • Oral questioning • Interviewing • Portfolio of evidence • Third party report

	• Resources utilization • Setting work priorities • Developing healthy relationships • HIV and AIDS • Drug and substance abuse • Managing emerging issues	
4. Lead a workplace team	• Leadership qualities • Power and authority • Team building • Determination of team roles and objectives • Team parameters and relationships • Individual responsibilities in a team • Forms of communication • Complementing team activities • Gender and gender mainstreaming • Human rights • Developing healthy relationships • Maintaining relationships • Conflicts and conflict resolution • Coaching and mentoring skills	• Written tests • Oral questioning • Interviewing • Portfolio of evidence • Third party report
5. Plan and organize work	• Functions of management • Planning • Organizing • Time management • Decision making concept • Task allocation • Developing work plans • Developing work goals/objectives and deliverables • Monitoring work activities • Evaluating work activities • Resource mobilization • Resource allocation • Resource utilization	• Written tests • Oral questioning • Interviewing • Portfolio of evidence • Third party report

	• Proactive planning • Risk evaluation • Problem solving • Collecting, analysing and organising information • Negotiation	
6. Maintain professional growth and development	• Avenues for professional growth • Training and career opportunities • Assessing training needs • Mobilizing training resources • Licenses and certifications for professional growth and development • Pursuing personal and organizational goals • Managing work priorities and commitments • Recognizing career advancement	• Written tests • Oral questioning • Interviewing • Portfolio of evidence • Third party report
7. Demonstrate workplace learning	• Managing own learning • Mentoring • Coaching • Contributing to the learning community at the workplace • Cultural aspects of work • Networking • Variety of learning context • Application of learning • Safe use of technology • Taking initiative/proactivity • Flexibility • Identifying opportunities • Generating new ideas • Workplace innovation • Performance improvement • Managing emerging issues • Future trends and concerns in learning	• Written tests • Oral questioning • Interviewing • Portfolio of evidence • Third party report

8. Demonstrate problem solving skills	• Critical thinking process • Data analysis tools • Decision making • Creative thinking • Development of creative, innovative and practical solutions • Independence in identifying and solving problems • Solving problems in teams • Application of problem-solving strategies • Testing assumptions • Resolving customer concerns	• Written tests • Oral questioning • Interviewing • Portfolio of evidence • Third party report
9. Manage ethical performance	• Meaning of ethics • Ethical perspectives • Principles of ethics • Ethical standards • Organization code of ethics • Common ethical dilemmas • Organization culture • Corruption, bribery and conflict of interest • Privacy and data protection • Diversity, harassment and mutual respect • Financial responsibility/accountability • Etiquette • Personal and professional integrity • Commitment to jurisdictional laws • Emerging issues in ethics	• Written tests • Oral questioning • Interviewing • Portfolio of evidence • Third party report

Suggested Methods of Instruction

- ❑ Demonstrations
- ❑ Simulation/Role play
- ❑ Group Discussion
- ❑ Presentations

- ❑ Assignments
- ❑ Q&A

Recommended Resources

- Computers
- Stationery
- Charts
- Video clips
- Audio tapes
- Radio sets
- TV sets
- LCD projectors

ENVIRONMENTAL LITERACY

UNIT CODE: SEC/CU/CS/BC/05/6/A

Relationship to Occupational Standards:
This unit addresses the Unit of Competency : Demonstrate Environmental Literacy

Duration of Unit: 40 hours

Unit Description
This unit describes the competencies required demonstrate environmental literacy.it involves controlling environmental hazard, controlling environmental pollution, complying with workplace sustainable resource use, evaluating current practices in relation to resource usage, identifying environmental legislations/conventions for environmental concerns, implementing specific environmental programs, monitoring activities on environmental protection/programs, analysing resource use and developing resource conservation plans.

Summary of Learning Outcomes
1. Control environmental hazard
2. Control environmental Pollution
3. Demonstrate sustainable resource use
4. Evaluate current practices in relation to resource usage
5. Identify Environmental legislations/conventions for environmental concerns
6. Implement specific environmental programs
7. Monitor activities on Environmental protection/Programs
8. Analyze resource use
9. Develop resource conservation plans

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Control environmental hazard	• Purposes and content of Environmental Management and Coordination Act 1999 • Storage methods for environmentally hazardous materials • Disposal methods of hazardous wastes • Types and uses of PPE in line with environmental regulations	• Written questions • Oral questions

	• Occupational Safety and Health Standards (OSHS)	
2. Control environmental Pollution control	• Types of pollution • Environmental pollution control measures • Types of solid wastes • Procedures for solid waste management • Different types of noise pollution • Methods for minimizing noise pollution	• Written questions • Oral questions • Role play
3. Demonstrate sustainable resource use	• Types of resources • Techniques in measuring current usage of resources • Calculating current usage of resources • Methods for minimizing wastage • Waste management procedures • Principles of 3Rs (Reduce, Reuse, Recycle) • Methods for economizing or reducing resource consumption	• Written questions • Oral questions • Role play
4. Evaluate current practices in relation to resource usage	• Collection of information on environmental and resource efficiency systems and procedures, • Measurement and recording of current resource usage • Analysis and recording of current purchasing strategies. • Analysis of current work processes to access information and data • Identification of areas for improvement	• Written questions • Oral questions • Role play
5. Identify Environmental legislations/conventions for environmental concerns	• Environmental issues/concerns • Environmental legislations /conventions and local ordinances • Industrial standard /environmental practices	• Written questions • Oral questions

	• International Environmental Protocols (Montreal, Kyoto) • Features of an environmental strategy	
6. Implement specific environmental programs	• Community needs and expectations • Resource availability • 5s of good housekeeping • Identification of programs/Activities • Setting of individual roles /responsibilities • Resolving problems /constraints encountered • Consultation with stakeholders	• Written questions • Oral questions • Role play
7. Monitor activities on Environmental protection/Programs	• Periodic monitoring and Evaluation of activities • Gathering feedback from stakeholders • Analyzing data gathered • Documentation of recommendations and submission • Setting of management support systems to sustain and enhance the program • Monitoring and reporting of environmental incidents to concerned /proper authorities	• Oral questions • Written tests • Practical test
8. Analyze resource use	• Identification of resource consuming processes • Determination of quantity and nature of resource consumed • Analysis of resource flow through different parts of the process. • Classification of wastes for possible source of resources.	• Written tests • Oral questions • Practical test

9. Develop resource Conservation plans	• Determination of efficiency of use/conversion of resources • Causes of low efficiency of use of resources • Plans for increasing the efficiency of resource use	• Written tests • Oral questions • Practical test

Suggested Methods of Instruction

- Instructor led facilitation of theory
- Practical demonstration of tasks by trainer
- Practice by trainees
- Observations and comments and corrections by trainers

Recommended Resources

- Standard operating and/or other workplace procedures manuals
- Specific job procedures manuals
- Environmental Management and Coordination Act 1999
- Machine/equipment manufacturer's specifications and instructions
- Personal Protective Equipment (PPE)
- ISO standards
- Company environmental management systems (EMS)
- Montreal Protocol
- Kyoto Protocol

OCCUPATIONAL SAFETY AND HEALTH PRACTICES

UNIT CODE: SEC/CU/CS/BC/06/6/A

Relationship to Occupational Standards
This unit addresses the Unit of Competency: Demonstrate Occupational Safety and Health Practices

Duration of Unit: 40 hours

Unit Description
This unit specifies the competencies required to demonstrate occupational health and safety practices. It involves identifying workplace hazards and risk, identifying and implementing appropriate control measures to hazards and risks and implementing OSH programs, procedures and policies/guidelines.

Summary of Learning Outcomes
1. Identify workplace hazards and risk
2. Control OSH hazards
3. Implement OSH programs

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Identify workplace hazards and risks	• Identification of hazards in the workplace and/or the indicators of their presence • Evaluation and/or work environment measurements of OSH hazards/risk existing in the workplace • Gathering of OSH issues and/or concerns	• Oral questions • Written tests • Portfolio of evidence • Third party report
2. Control OSH hazards	• Prevention and control measures e.g. use of PPE • Risk assessment • Contingency measures	• Oral questions • Written tests • Portfolio of evidence • Third party report
3. Implement OSH programs	• Company OSH program, evaluation and review • Implementation of OSH programs	• Oral questions • Written tests • Portfolio of

	• Training of team members and advice on OSH standards and procedures • Implementation of procedures for maintaining OSH-related records	evidence • Third party report

Suggested Methods of Instruction

- Assigments
- Discussion
- Q&A
- Role play
- Viewing of related videos

Recommended Resources

- Standard operating and/or other workplace procedures manuals
- Specific job procedures manuals
- Machine/equipment manufacturer's specifications and instructions
- Personal Protective Equipment (PPE) e.g.
    - Mask
    - Face mask/shield
    - Safety boots
    - Safety harness
    - Arm/Hand guard, gloves
    - Eye protection (goggles, shield)
    - Hearing protection (ear muffs, ear plugs)
    - Hair Net/cap/bonnet
    - Hard hat
    - Face protection (mask, shield)
    - Apron/Gown/coverall/jump suit
    - Anti-static suits
    - High-visibility reflective vest

COMMON UNITS OF LEARNING

DIGITAL LITERACY

UNIT CODE: SEC/CU/CS/CC/01/6/A

Relationship to Occupational Standards
This unit addresses the Unit of Competency: Demonstrate digital literacy

Duration of Unit: 70 hours

Unit Description
This unit covers the competencies required to demonstrate digital literacy. It involves identify appropriate computer software and hardware, applying security measures to data, hardware, and software in automated environment, computer software in solving tasks, internet and email in communication at workplace, desktop publishing in official assignments and preparing presentation packages.

Summary of Learning Outcomes
1. Identify computer software and hardware
2. Apply security measures to data, hardware and software
3. Apply computer software in solving tasks
4. Apply internet and email in communication at workplace
5. Apply desktop publishing in official assignments
6. Prepare presentation packages

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Identify computer hardware and software	• Concepts of ICT • Functions of ICT • History of computers • Components of a computer • Classification of computers	• Written tests • Oral presentation • Observation
2. Apply security measures to data, hardware and software	• Data security and control • Security threats and control measures • Types of computer crimes • Detection and protection against computer crimes	• Written tests • Oral presentation • Observation • Project

	• Laws governing protection of ICT	
3. Apply computer software in solving tasks	• Operating system • Word processing • Spread sheets • Data base design and manipulation • Data manipulation, storage and retrieval	• Oral questioning • Observation • Project
4. Apply internet and email in communication at workplace	• Computer networks • Network configurations • Uses of internet • Electronic mail (e-mail) concept	• Oral questioning • Observation • Oral presentation • Written report
5. Apply desktop publishing in official assignments	• Concept of desktop publishing • Opening publication window • Identifying different tools and tool bars • Determining page layout • Opening, saving and closing files • Drawing various shapes using DTP • Using colour pellets to enhance a document • Inserting text frames • Importing and exporting text • Object linking and embedding • Designing of various publications • Printing of various publications	• Oral questioning • Observation • Oral presentation • Written report • Project
6. Prepare presentation packages	• Types of presentation packages • Procedure of creating slides • Formatting slides • Presentation of slides • Procedure for editing objects	• Oral questioning • Observation • Oral presentation • Written report • Project

Suggested Methods of instructions

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

- Group discussions

Recommended Resources

- Desk top computers
- Laptop computers
- Other digital devices
- Printers
- Storage devices
- Internet access
- Computer software

CORE UNITS OF LEARNING

COMPUTER REPAIR AND MAINTENANCE

UNIT CODE: SEC/CU/CS/CR/01/6/A

Relationship to Occupational Standards
This unit addresses the unit of competency: Perform computer repair and maintenance

Duration of Unit: 120 hours

Unit Description
This unit covers the competencies required to perform computer repair and maintenance. It involves performing troubleshooting, dismantling faulty components, repairing/replacing faulty components, upgrading computer software/hardware, and preparing and documenting maintenance reports.

Summary of Learning Outcomes

1. Perform troubleshooting
2. Dismantle faulty components
3. Repair/Replace faulty components
4. Upgrade computer hardware/software
5. Prepare and document maintenance report

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods

1. Perform troubleshooting	• Meaning terms
	• Fundamentals of computer operations
	• Factors affecting computers performance
	  • Hardware
	  • Software
	• Computer testing
	• Tools used in computer testing
	  • Software
	  • Hardware
		• Written tests
		• Oral questioning
		• Observation
		• Practical tests

Learning Outcome	Content	Suggested Assessment Methods

2. Dismantle faulty components	• Meaning of terms
	• Computer dismantling tools
	• Computer components and dismantling procedures
	• Handling of computer components
	• Safety precautions
	  • Hardware
	  • Software
	  • Personnel
		• Written tests
		• Observation
		• Oral questioning
		• Practical tests

3. Repair/Replace faulty components	• Meaning of terms
	• Computer diagnostic procedures
	  • Tools and instruments used in computer diagnosis process
	• Procedures in repair/ replacements of computer components
	• Testing and replacements of repaired/replaced computer components
	• Procedures in computer repair
	  • Hardware
	  • Software
	• Assembling of computer components
		• Written tests
		• Observation
		• Oral questioning
		• Practical tests

4. Upgrade and update computer hardware/software	• Meaning of terms • Procedures in updating and upgrading computer software and hardware • Software and hardware licensing procedure • Testing of upgraded and updated computer hardware and software	• Written tests • Observation • Oral questioning • Practical tests
5.Prepare and document maintenance report	• Preparation of maintenance report • Sharing of maintenance report • Filing of maintenance report	• Observation • Oral questioning • Practical tests • Written tests

Suggested Methods of Instructions

- Demonstration by trainer
- Practice by the trainee
- Field trips

- On-job-training
- Discussions

Recommended Resources

Tools	**Materials and supplies**
• Measuring tools • Hardware and software diagnostic tools	• Stationery • Assorted Cables • Assorted protective devices • Accessories
Equipment	**Reference materials**
• Computer • Printers • Monitors • Projectors	• Standards • Internet • Organization ICT polices • Occupational Safety and Health Act (OSHA) • National Environmental Management Authority (NEMA) regulations • National Construction Authority (NCA) regulations • Tables

CYBER SECURITY LAWS, POLICIES AND REGULATIONS

UNIT CODE: SEC/CU/CS/CR/02/6/A

Relationship to Occupational Standards
This unit addresses the unit of competency: Apply cyber security laws, policies and regulations

Duration of Unit: 190 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

1. Demonstrate understanding of cyber security laws, policies and regulations
2. Develop Cyber Security policy
3. Implement Cyber Security policy and regulations
4. Evaluate Cyber security policy
5. Evaluate compliance in Cyber security policy and regulations
6. Monitor effectiveness of Cyber security policy in an organization

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods

1. Demonstrate understanding of cyber security laws	• Meaning of terms
	  • World legal system e.g
	  • Common law
	  • Religious law
	  • Hindu law
	  • Islamic law
	• Types of Cyber security laws
	  • National
	  • International
	• Cyber crimes
	  • Types of cyber crimes
	  • Challenges in prosecuting cyber crime
		• Observation
		• Oral questioning
		• Written tests
		• Practical tests

Learning Outcome	Content	Suggested Assessment Methods

	• Cyber-crime laws
	  • Local Cyber crime laws
	  • International Cyber crime laws
	• Application of cyber security laws
	• Compliance of cyber security laws
	• Impacts of cyber crime
	  • Positive and Negative	

2. Demonstrate understanding of different Cyber security policies and regulations	• Meaning of terms • Fundamentals of cyber security • Types of cyber security policies and regulation • Application of different cyber security policies • Stakeholders involved in cyber security policies and regulations • Regulatory board in cyber security policies	• Observation • Oral questioning • Written tests • Practical tests
3. Develop Cyber Security policy	• Meaning of terms • Components of cyber security and information classification • Cyber security policy alignments to the vision and mission • Procedures of drafting cyber security policy • Cyber security review process	• Observation • Oral questioning • Written tests • Practical tests
4. Implement Cyber Security policy and regulations	• Meaning of terms • Cyber security policy implementation process • Cyber security policy implementation team • Importance of schedule in the implementation process of cyber security policy • Verification of cyber security implementation • Relevant regulations in implementation of cyber security policy	• Observation • Oral questioning • Written tests • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
5. Evaluate Cyber security policy	• Meaning of terms • Review and updates of cyber security policy • Process of evaluation of cyber security policy • Factors to consider in evaluation of cyber security policy	• Observation • Oral questioning • Written tests • Practical tests
6. Evaluate compliance in Cyber security policy and regulations	• Meaning of terms • Infrastructure and landscape audit • Calculation of risk factors • Calculation of non – compliance factors • Compliance level recommendation	• Observation • Oral questioning • Written tests • Practical tests

7. Monitor effectiveness of Cyber security policy in an organization	• Meaning of terms
	• Compliance level
	• Cyber security policy monitoring impact on:
	  • Process
	  • People
	  • Technology
	• Monitoring effectiveness of cyber security policy
		• Observation
		• Oral questioning
		• Written tests
		• Practical tests

Suggested Methods of Instructions

- Discussions
- Site visits
- On-job-training
- Charts and Audio-visual presentations
- Templates

Recommended Resources

Equipment	Reference materials
• Computers • Printers • Cameras • Phones	• Internet • NIST Cyber security framework • Constitution • Cyber crime 2018
Materials and supplies	**Tools**

• Stationery	Framework

COMPUTER NETWORKING

UNIT CODE: SEC/CU/CS/CR/03/6/A

Relationship to Occupational Standards
This unit addresses the unit of competency: Perform computer networking

Duration of Unit: 130 hours

Unit Description
This unit covers the competencies required to perform computer networking activities. 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

1. Identify network type
2. Configure network devices
3. Connect network devices
4. Monitor Network performance
5. Document network report
6. Train network users
7. Maintain Network

Learning Outcomes, Content and Suggested Assessment Methods:

Learning Outcome	Content	Suggested Assessment Methods
1. Identify network type	• Meaning of terms • Network components • Network design and architecture • Types of network topology	• Written tests • Oral questioning • Practical tests • Observation
2. Configure network devices	• Meaning of terms • Network configuration • Types of network protocols • Network segmentation • Network privileges • Network connections	• Written tests • Oral questioning • Practical tests • Observation

3. Connect network devices	• Meaning of Terms • Tools used in network devices ❑ Importance of termination • Stability and connectivity of the network • Cable Management	• Written tests • Oral questioning • Practical tests • Observation
4. Monitor Network performance	• Meaning of teams • Monitoring tools in network performance • Deployment of network monitoring tools • Monitoring network status • Network operation manual	• Written tests • Oral questioning • Practical tests • Observation
5. Document network report	• Meaning of terms • Preparation of networking report • Report sharing • Report filing	• Written tests • Oral questioning • Practical tests • Observation
6. Train network users	• Meaning of terms • Identification and training of network users. • Preparation of network training manuals	• Written tests • Oral questioning • Practical tests • Observation
7. Maintain Network	• Meaning of terms • Network optimization • Network vulnerability and security • Preparation of network maintenance schedule and updates	• Written tests • Oral questioning • Practical tests • Observation

Suggested Methods of Instructions

- Projects
- Demonstration by trainer
- Practice by the trainee
- Field trips
- On-job training
- Discussions

Recommended Resources

Tools and equipment	**Materials and supplies**
• Cable Strippers • Pliers • Screw drivers • Chisels • Crimping tools • Personal protective equipment • Computers	• Stationery • Cables • Accessories • Cable trays • Cable ducts • Trunkings • Screws
Reference materials • Occupational safety and health act (OSHA) • Work injury benefits act(WIBA) • Manufacturers' catalogues • British standards • KEBS standards • Tables	

BUILDING SECURE NETWORK

UNIT CODE: SEC/CU/CS/CR/04/6/A

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 confirming user requirements and network equipment, 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 preparing network report.

Summary of Learning Outcomes

1. Confirm user requirements and network equipment
2. Review security issues
3. Analyse network security protocols and features
4. Plan and design perimeter solution
5. Install and configure perimeter solutions
6. Configure internal network devices
7. Test and verify design performance
8. Prepare network report

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Confirm user requirements and network equipment	• Meaning of terms • Uses of network • Network requirements and equipment • Network topology • Network perimeters and bandwidth • Security perimeter	• Observation • Oral questioning • Written tests • Practical tests
2. Review security issues	• Meaning of terms • Network threats • Threats and vulenerablilties identification • Factors to consider in reviewing security	• Observation • Oral questioning • Written tests • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	issues • Identification and selection of security control measures	
3. Analyse network security protocols and features	• Meaning of terms • Types of network security protocols and standards • Application of network security protocols and standards • Factors to consider in network security protocol analysis	• Observation • Oral questioning • Written tests • Practical tests
4. Plan and design perimeter solution	• Meaning of terms • Factors to consider in designing perimeter solution • Designing perimeter schedule • Approval of perimeter schedule • Testing of perimeter design • Simulation of perimeter design	• Observation • Oral questioning • Written tests • Practical tests
5. Install and configure perimeter solutions	• Meaning of Terms • Factors to consider in acquiring perimeter solutions • Factors to consider in installation of perimeter solution • Configuration of perimeter solutions • Testing of perimeter solution	• Observation • Oral questioning • Written tests • Practical tests
6. Configure internal network devices	• Meaning of terms • Factors to consider in configuration of internal network devices • Types of internal network devices • Internal network devices compatibility tests • Integration of internal devices with security perimeter	• Observation • Oral questioning • Written tests • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
7. Test and verify design performance	• Meaning of terms • Types of tests • System performance tests • Checking and debugging of errors • Threats simulation tests • Monitoring of security perimeter	• Observation • Oral questioning • Written tests • Practical tests
8. Prepare network report	• Meaning of terms • Preparation of networking report • Report dissemination • Report filing	• Observation • Oral questioning • Written tests

Suggested Methods of Instructions

- Discussions
- Site visits
- On-job-training
- Charts and Audio-visual presentations

Recommended Resources

Equipment	Reference materials
• Computers • Printers • Cameras • Phones	• Manufacturers' catalogues • EMCA Act • OSHA • County by-laws
Materials and supplies • Stationery	

SOFTWARE DEVELOPMENT

UNIT CODE: SEC/CU/CS/CR/05/6/A

Relationship to Occupational Standards
This unit addresses the unit of competency: Develop computer software

Duration of Unit: 130 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.

Summary of Learning Outcomes

1. Establish software purpose
2. Analyse software requirement
3. Design computer software
4. Develop computer software
5. Perform programme testing
6. Perform software maintenance

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods

1. Establish software purpose	• Meaning of term
	• Software classification
	  • Factors to consider in software classification
	• Software functionality
	• Software selection
	  • Factors consider in software selection
	• Software acquisition method
		• Observation
		• Oral questioning
		• Written tests
		• Practical tests

2. Analyse software requirement	• Meaning of terms • Software specification • Computer resources • Software installation platform • User vendor agreement	• Observation • Oral questioning • Written tests • Practical tests
3. Design computer software	• Meaning of terms • Software design specifications • Factors to consider in software design	• Observation • Oral questioning • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	• Software life cycle • Integration of security in software design • Software installation devices • Software parameters	• Written tests
4. Develop computer software	• Meaning of terms • Factors to consider in software development • Software coding • Testing and debugging of software errors • Software development requirements • User task analysis	• Observation • Oral questioning • Written tests • Practical tests

5. Perform programme testing	• Meaning of terms
	• Types of tests
	  • Software functionality testing
	  • Software security testing
	• Software debugging
	• Configuration testing
	• Software reporting and testing
	• Quality assurance and testing
	• User acceptance and implementation
		• Observation
		• Oral questioning
		• Written tests
		• Practical tests

6. Perform software maintenance	• Meaning of terms • Preparation of software maintenance schedule • Software patch management • Software version control • Software review • Software monitoring and evaluation	• Observation • Oral questioning • Written tests • Practical tests

Suggested Methods ofInstructions

- Demonstration by trainer
- Practice by the trainee
- Field trips
- Discussions

Recommended Resources

• Computers • Printers	**Materials and supplies** • Stationery

• Cameras • Phones • Photocopiers	•
Reference materials • Manufacturers' manuals • Relevant catalogues • Tables • National and international standards	

SOFTWARE APPLICATION SECURITY

UNIT CODE: SEC/CU/CU/CR/06/6/A

Relationship to Occupational Standards
This unit addresses the unit of competency: Secure software application

Duration of Unit: 110 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, performing application security configuration and preparation of reports on software security.

Summary of Learning Outcomes

1. Identify software to be secured
2. Establish tools for application security assessment
3. Perform application security assessment
4. Harden software application
5. Monitor application security performance
6. Prepare a report on software security

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Identify software to be secured	• Meaning of Terms • Types of software • Classification of software and their application • Factors influencing software selection • Software operation platform	• Observation • Written tests • Oral questioning • Practical tests

2. Establish tools for application security assessment	• Meaning of terms
	• Types of tools used in software application security assessment
	  • Network communication in tools selection
	• Platform vulnerability
	• Factors to consider in selection security assessment tools
	  • Tool data size in tools selection
		• Observation
		• Written tests
		• Oral questioning
		• Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	• Environment • Software and Hardware	
3. Perform application security assessment	• Meaning of terms • Types of known standards in application security assessment • Best practice standards in application security assessment	• Observation • Written tests • Oral questioning • Practical tests
• Harden software application	• Meaning of terms • Software configuration • Factors to consider in software hardening • Policies and regulations software hardening • Security measures in software application • Elements of security in software hardening • Licenses in software installation • Software monitoring process • Installation of patches, upgrades and updates in software hardening • Purposes of environment in software hardening	• Observation • Written tests • Oral questioning • Practical tests
5. Monitor application security performance	• Meaning of terms • Factors to consider in monitoring of application security performance • Implementation of monitoring solutions • Logs management and monitoring • Measurement of application security performance	• Observation • Written tests • Oral questioning • Practical tests
6. Prepare a report on software security	• Meaning Testing • Report preparation • Report dissemination • Report filing	• Observation • Written tests • Oral questioning • Practical tests

Suggested Methods of Instructions

- Demonstration by trainer
- Practice by the trainee
- Discussions

Recommended Resources

Equipment	**Materials and supplies**
• Computers • Printers • Cameras • Phones • Photocopiers	• Stationery •
Reference materials • Manufacturers' manuals • Relevant catalogues • Tables • National and international standards	

DATABASE SECURITY

UNIT CODE: SEC/CU/CS/CR/07/6/A

Relationship to Occupational Standards
This unit addresses the unit of competency: Secure database

Duration of Unit: 72 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 database security management system, monitoring database security, monitoring access control and managing database backups.

Summary of Learning Outcomes

1. Identify types of databases
2. Identify database threats and vulnerabilities
3. Install databases patches
4. Install database security management systems
5. Monitor database security
6. Manage access control
7. Manage database backups

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Identify types of databases	• Meaning of terms • Types of databases • Classification of databases • Database management system • Database concurrence • Database operational model and cost evaluation	• Written tests • Oral questioning • Observation • Practical tests
2. Identify database threats and vulnerabilities	• Meaning of terms • Database testing • Factors to consider in database testing • Types of database threats and vulnerabilities • Assessment of security vulnerabilities, risk	• Written tests • Oral questioning • Observation • Practical tests

	and threats in database	

3. Install databases patches	• Meaning of terms
	• Factors to consider in installation of security patches
	• Database patches management
	  • Identification
	  • Verification
	  • Monitoring
	  • Deployment
	• Environment in installation of database patches
		• Observation
		• Oral questioning
		• Practical tests
		• Written tests

4. Install database security management systems	• Meaning of terms • Identification of database of database security management system • Deployment model in database security management system • Types of deployment models • Hardware sizing in database • Configuration and verification of database security management system • Integration of database security management system	• Observation • Oral questioning • Practical tests • Written tests
5. Monitor database security	• Meaning of terms • Logs collection, analysis and correlation • Logs management Failed logs Odd hours • Security control in log management	• Observation • Oral questioning • Practical tests • Written tests
6. Manage access control	• Meaning of terms • Factors to consider in management of database access control system • Implementation, management and monitoring of database access control management system • Database auditing system	• Observation • Oral questioning • Practical tests • Written tests

7. Manage database backups	• Meaning of terms • Development of backup strategy • Identification database backup solutions • Implement database back up management system • ICT policy in management of database backups • Synchronization of database back up • Monitoring, testing and auditing of database backups • Storage of database backups	• Written tests • Oral questioning • Observation • Practical tests

Suggested Methods of instructions

- Demonstration by trainer
- Practice by the trainee
- Field trips
- On-job-training
- Discussions

Recommended Resources

Equipment	**Materials and supplies**
• Computers • Printers • Cameras • Phones • Photocopiers	• Stationery
Reference materials • Manufacturers' manuals • Relevant catalogues • Tables • National and international standards	

INSTALLATION OF CYBER SECURITY SYSTEM

UNIT CODE: SEC/CU/CU/CR/08/6/A

Relationship to Occupational Standards
This unit addresses the unit of competency: Install Cyber security system

Duration of Unit: 130 hours

Unit Description

This unit covers the competencies required to Install cyber security system. It involves identifying and analysing information to be protected, establishing systems to be installed, assessing system compatibility, installing established systems, performing system testing and debugging, monitoring system performance, documenting system installation report, establishing a cyber security backup and restoration plan and conducting training of the system users.

Summary of Learning Outcomes

1. Identify and analyze information to be protected
2. Establish systems to be installed
3. Asses system's compatibility
4. Install established systems
5. Perform systems testing and debugging
6. Monitor system performance
7. Document system installation report
8. Establish a cyber-security back up and restoration plan
9. Conduct training of system users

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Identify and analyze information to be protected	• Meaning of terms • Establishment of information platforms • Determination of information attributes	• Observation • Written tests • Oral questioning

	• Technology in information storage and analysis • Information access control • Information analysis	• Practical tests
2. Establish systems to be installed	• Meaning of terms • Factors to consider in establishment of cyber security system • Trends and threats in security system • Hardware and software requirement is security system installation	• Observation • Written tests • Oral questioning • Practical tests
3. Asses system's compatibility	• Meaning of terms • Compatibility assessment of cyber security system • Factors to consider in assessment of cyber security system compatibility • Components specification in system assessment • Procedures of cyber security system assessment	• Observation • Oral questioning • Practical tests • Written tests
4. Install established systems	• Meaning of terms • Acquisition of cyber security management system • Tools in installation of cyber security system • System installation scheduling • Cyber security system configuration	• Observation • Oral questioning • Practical tests • Written tests
5. Perform systems testing and debugging	• Meaning of terms • Types of tests on a cyber-security system • Factors to consider in testing and debugging of cyber security system • Testing process of the cyber security system • Debugging and error troubleshooting	• Observation • Oral questioning • Practical tests • Written tests
6. Monitor system performance	• Meaning of terms • System monitoring process • System simulation • Logs auditing • Patch management	• Observation • Oral questioning • Practical tests • Written tests

7. Document system installation report	• Meaning of terms • Report preparation • Report dissemination • Report filing	• Observation • Written tests • Oral questioning • Practical tests

8. Establish a Cyber security back up and restoration plan	• Meaning of terms
	• Establishment of cyber security back up management system
	• Factors to consider in establishment of cyber security system
	  • Information in cyber security back up and restoration plan
	• Backup media and process
	• Back up testing
	  • Validation
	  • Performance
	  • Integrity
	• Back up procedures
		• Observation
		• Written tests
		• Oral questioning
		• Practical tests

9. Conduct training of system users	• Meaning of terms • Cyber security system user training preparation • Training manuals are prepared • Filing of cyber security system operation manual	• Observation • Written tests • Oral questioning • Practical tests

Suggested Methods of Instruction

- Demonstration by trainer
- Practice by the trainee
- Field trips
- On-job-training
- Discussions

Recommended Resources

Equipment	Materials and supplies
• Computers • Printers • Cameras • Phones • Photocopiers	• Stationery

Reference materials • Manufacturers' manuals • Relevant catalogues • Tables • National and international standards	

MANAGEMENT OF CYBER SECURITY RISKS

UNIT CODE: SEC/CU/CS/CR/09/6/A

Relationship to Occupational Standards
This unit addresses the unit of competency: Manage Cyber security risks

Duration of Unit: 120 hours

Unit Description
This unit covers the competencies required to manage cyber security risks. It involves establishing risk context, identify risk factors, implementing contingency plans, monitoring and updating risk profiles and reporting of risk profiles.

Summary of Learning Outcomes

1. Establish Risk context
2. Identify Risk factors
3. Implement contingency plans
4. Monitor and update risk profile
5. Report risk profile

Learning Outcomes, Content and Suggested Assessment Methods:

Learning Outcome	Content	Suggested Assessment Methods
1. Establish Risk context	• Meaning of terms • Assets inventory • Assets classification • Types of assets • Security awareness • Organization risk appetite	• Observation • Written tests • Oral questioning • Practical tests
2. Identify Risk factors	• Meaning of terms • Risks factors identification • Factors to consider in risks factors identification • Risk factors assessment • Risk factor analysis • Classification of risk factors • Assessment of information access ability	• Observation • Written tests • Oral questioning • Practical tests

3. Implement contingency plans	• Meaning of terms • Implementation backup strategy • Data loss prevention measures • Contingency plans communication strategy • IDS/IPS implementations • Simulation of contingency plans	• Observation • Written tests • Oral questioning • Practical tests
4. Monitor and update risk profile	• Meaning of terms • Risk calculation • Implementation of security operation centres for threat monitoring • SOC operators training • Risk profile update	• Observation • Written tests • Oral questioning • Practical tests
5. Report risk profile	• Meaning of terms • Report preparation • Report dissemination • Report filing	• Observation • Written tests • Oral questioning • Practical tests

Suggested Methods of Instructions

- Projects
- Demonstration by trainer
- Practice by the trainee
- Field trips
- On-job training
- Discussions

Recommended Resources

Equipment	**Materials and supplies**
• Computers • Printers • Cameras • Phones • Photocopiers	• Stationery
Reference materials • Manufacturers' manuals • Relevant catalogues • Tables	

• National and international standards	

CYBER SECURITY ASSESSMENT AND TESTING

UNIT CODE: SEC/CU/CS/CR/10/6/A

Relationship to Occupational Standards
This unit addresses the unit of competency: Conduct cyber security assessment and testing

Duration of Unit: 110 hours

Unit Description
This unit covers the competencies required to conduct 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

1. Gather information about organization and its systems
2. Scan and map the network
3. Enumerate target resources
4. Exploit known vulnerabilities
5. Perform social engineering
6. Prepare security assessment and testing report

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods

1. Gather information about organization and its systems	• Meaning of terms
	• Information gathering and reconnaissance
	• Methods of information gathering
	  • Social engineering
	  • Search engines
	• Target mapping
	• Organization operation structures
		❑ Observation
		❑ Written tests
		❑ Oral questioning
		❑ Practical tests

2. Scan and map the network	• Meaning of terms • Probing and scanning • Drawing network topology • Services enumeration • Vulnerability assessment	• Observation • Written tests • Oral questioning • Practical tests
3. Enumerate target	• Meaning of terms	• Observation

Learning Outcome	Content	Suggested Assessment Methods
resources	• User identification and log in credentials • Service, protocol ,workgroup and database enumeration • Password cracking	• Oral questioning • Practical tests • Written tests
4. Exploit known vulnerabilities	• Meaning of terms • Payload preparation and deployment • Deploying methods • Deployment of exploits • Access to remote hosts maintenance • Proof of concepts	• Observation • Written tests • Oral questioning • Practical tests
5. Perform social engineering	• Meaning of terms • Information gathering • Social engineering technics • User and system manipulation	• Observation • Written tests • Oral questioning • Practical tests
6. Prepare security assessment and testing report	• Meaning of terms • Report preparation • Report dissemination • Report filing	• Observation • Written tests • Oral questioning • Practical tests

Suggested Methods of Instruction

- Demonstration by trainer
- Practice by the trainee
- Field trips
- Discussions

Recommended Resources

Equipment	Materials and supplies
• Computers • Printers • Cameras • Phones • Photocopiers	• Stationery
Reference materials • Manufacturers' manuals • Relevant catalogues • Tables	

• National and international standards	

MANAGEMENT OF SECURITY OPERATIONS

UNIT CODE: SEC/CU/CS/CR/11/6/A

Relationship to Occupational Standards
This unit addresses the unit of competency: Manage security operations

Duration of Unit: 110 hours

Unit Description
This unit covers the competencies required to manage security operations. It involves gathering information asset inventory, implementing a security management solution, establishing threats landscape, responding to established threats, monitoring events in the landscape and generating security operation report.

Summary of Learning Outcomes

1. Gather information asset inventory
2. Implement a security management solution
3. Establish threats landscape
4. Respond to established threats
5. Monitor events in the landscape
6. Generate security operations report

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Gather information about organization and its systems	• Meaning of terms • Information assets inventory • Determination of asset value • Classification of information assets	• Observation • Oral questioning • Practical tests • Written tests
2. Implement a security management solution	• Meaning of terms • Acquisition of security management system • Security management solution deployment • Security management configuration • Security management system hardening • Dashboard/Portal configuration	• Observation • Oral questioning • Practical tests • Written tests
3. Establish threats landscape	• Meaning of terms • Threats identification and modelling • Threat mitigation measures	• Observation • Oral questioning • Practical tests • Written tests

Learning Outcome	Content	Suggested Assessment Methods
4. Respond to identified threats	• Meaning of terms • Reporting procedure • Incidence handling and response • Business continuity plan	• Observation • Oral questioning • Practical tests • Written tests
5. Monitor security events in the landscape	• Meaning of team • SIEM implementation • Technical users awareness training • Updating, upgrading and patching of security management system • Simulation of threats and monitoring	• Observation • Oral questioning • Practical tests • Written tests
6. Generate security operations report	• Report preparation • Report dissemination • Report filing	• Observation • Oral questioning • Practical tests • Written tests

Suggested Methods of Instructions

- Demonstration by trainer
- Practice by the trainee
- Field trips
- Discussions

Recommended Resources

Equipments	Materials and supplies
• SOC • CERT • Computer • Mobile phone • Radio frequency receivers	• Stationery • Software and hardware • Cloud • Working platform
Reference materials • Internet • Manufacturers' manuals • Installation manuals • NIST cyber security framework framework • KE-CERT	