REPUBLIC OF KENYA

COMPETENCY BASED CURRICULUM

FOR

CYBER SECURITY LEVEL 5

TVET CDACC
P.O BOX 15745-00100
NAIROBI

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 (Sessional Paper No. 4 of 2016). 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 and the Sessional Paper No. 4 of 2016 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.

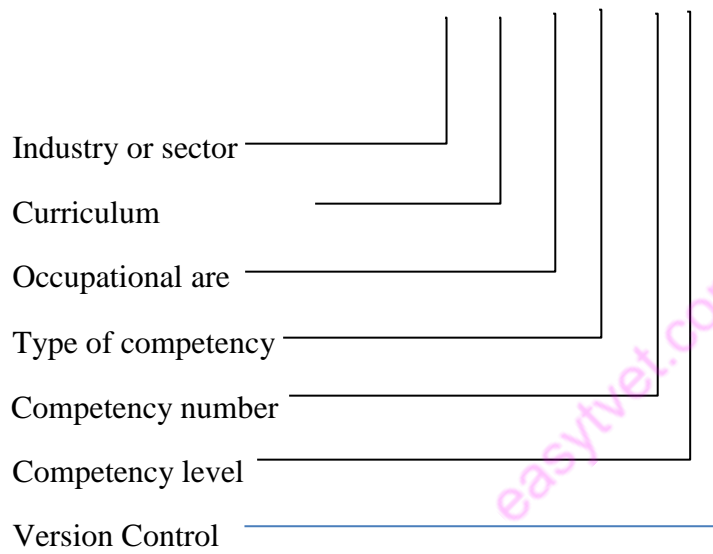**COUNCIL SECRETARY/CEO**
TVET CDACC

TABLE OF CONTENTS

ACRONYMNS AND ABBREVIATIONS

BC	Basic Competencies
CDACC	Curriculum Development, Assessment and Certification Council
CERT	Computer Emergency response team
CIRT	Computer Incidence response team
CR	Core Competencies
CS	Cyber Security
CU	Curriculum
EHS	Environment, Health and Safety
ENG	Engineering
IBMS	Integrated Building Management System
ICT	Information and communication Technology
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
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/01/5/A

Industry or sector

Curriculum

Occupational are

Type of competency

Competency number

Competency level

Version Control

OVERVIEW

Description of the course

This course is designed to equip a Cyber security operator 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 and security assessment and testing.

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/01/5/A	Communication skills	20	2
SEC/CU/CS/BC/02/5/A	Numeracy skills	30	3
SEC/CU/CS/BC/03/5/A	Entrepreneurial skills	80	8
SEC/CU/CS/BC/04/5/A	Employability skills	40	4
SEC/CU/CS/BC/05/5/A	Environmental literacy	20	2
SEC/CU/CS/BC/06/5/A	Occupational safety and health practices	30	3
Total		**220**	**22**

Common Units of Learning

Unit Code	Unit Title	Duration in Hours	Credit Factors
SEC/CU/CS/CC/01/5/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/01/5/A	Computer repair and maintenance	120	12
SEC/CU/CS/CR/02/5/A	Cyber security laws, policies and regulations	190	19
SEC/CU/CS/CR/03/5/A	Computer Networking	130	13
SEC/CU/CS/CR/06/5/A	Software application security	110	11
SEC/CU/CS/CR/07/5/A	Database Security	70	7
SEC/CU/CS/CR/08/5/A	Cyber security system administration	130	13
SEC/CU/CS/CR/10/5/A	Security Assessment and testing	110	11
	Industrial Attachment	480	48
Total		**1340**	**134**
Grand Total		**1,620**	**162**

The core units of learning are independent of each other and may be taken independently.

The total duration of the **course is 1,620 hours** (54 weeks at 30 hours per week) inclusive of industrial attachment.

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 D (plain)

Or

b) Level 4 certificate in a related course with **one** year of continuous work experience

Or

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

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

Industrial attachment

An individual enrolled in this course will be required to undergo an industrial attachment in a Cyber security firm for a period of at least 480 hours. Attachment will be undertaken upon completion of the course or the unit of learning.

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 operator Level 5, 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/01/5/A

Relationship to Occupational Standards

This unit addresses the Unit of Competency: Demonstrate Communication Skills

Duration of Unit: 25 hours

Unit Description

This unit covers the competencies required to demonstrate communication skills. It involves meeting communication needs of clients and colleagues, contributing to the development of communication strategies, conducting workplace interviews, facilitating group discussions and representing the organisation.

Summary of Learning Outcomes

1. Meet communication needs of clients and colleagues
2. Contribute to the development of communication strategies
3. Conduct interviews
4. Facilitate group discussions
5. 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 ❏ Effective questioning techniques (clarifying and probing) ❏ Workplace etiquette	❏ Interview ❏ Third party reports ❏ Written texts

	❑ Ethical work practices in handling communication ❑ Active listening ❑ Feedback ❑ Interpretation ❑ Flexibility in communication		
2. Contribute to the development of communication strategies	❑ Dynamics of groups ❑ Styles of group leadership ❑ Openness and flexibility in communication ❑ Communication skills relevant to client groups	❑ Written ❑ Observation	
3. Conduct interviews	❑ Types of interview ❑ Establishing rapport ❑ Facilitating resolution of issues ❑ Developing action plans	❑ Written ❑ Observation	
4. Facilitate group discussions	❑ Identification of communication needs ❑ Dynamics of groups ❑ Styles of group leadership ❑ Presentation of information ❑ Encouraging group members participation ❑ Evaluating group communication strategies	❑ Written ❑ Observation	
5. Represent the organization	❑ Presentation techniques ❑ Development of a presentation ❑ Multi-media utilization in presentation ❑ Communication skills relevant to client groups	❑ Observation ❑ Written	

Suggested Methods of Instruction
- Role playing
- Viewing of related videos

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

NUMERACY SKILLS

UNIT CODE: SEC/CU/CS/BC/02/5/A

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

Duration of Unit: 40 hours

Unit Description
This unit covers the competencies required to demonstrate numeracy skills. It involves calculating with whole numbers and familiar fractions, decimals, and percentages for work estimating, measuring, and calculating with routine metric measurements for work, using routine maps and plans for work, interpreting, drawing and constructing 2D and 3D shapes for work, interpreting routine tables, graphs and charts for work, collecting data and constructing routine tables and graphs for work and using basic functions of calculator

Summary of Learning Outcomes

1. Calculate with whole numbers and familiar fractions, decimals and percentages for work
2. Estimate, measure and calculate with routine metric measurements for work
3. Use routine maps and plans for work
4. Interpret, draw and construct 2D and 3D shapes for work
5. Interpret routine tables, graphs and charts for work
6. Collect data and construct routine tables and graphs for work
7. Use basic functions of calculator

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Calculate with whole numbers and familiar fractions, decimals and percentages for work	- Interpretation of whole numbers, fractions, decimals, percentages and rates - Calculations involving several steps - Calculation with whole numbers and routine or familiar fractions, decimals and percentages - Conversion between equivalent forms of fractions, decimals and percentages	- Written - Practical test - Observation

		• Application of order of operations to solve multi-step calculations • Application of problem solving strategies • Making estimations to check reasonableness of problem solving process, outcome and its appropriateness to the context and task • Use of formal and informal mathematical language and symbolism to communicate the result of a task	
2.	Estimate, measure and calculate with routine metric measurements for work	• Selection and interpretation of measurement information in workplace tasks and texts • Identification and selection of routine measuring equipment • Estimation and making measurements using correct units • Estimation and calculation using routine measurements • Performing conversions between routinely used metric units • Using problem solving processes to undertake tasks • Recording information using mathematical language and symbols	• Written • Practical test • Observation
3.	Use routine maps and plans 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	• Written • Practical test • Observation

		language	
4. Interpret, draw and construct 2D and 3D shapes for work	• Identify two dimensional shapes and routine three-dimensional 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 • Use formal and informal mathematical language to describe and compare common angles • Use common geometric instruments to draw two dimensional shapes • Construct routine three-dimensional objects from given nets	• Written • Practical test • Observation	
5. Interpret routine tables, graphs and charts for work	• Identify routine tables, graphs and charts in predominately familiar texts and contexts • Identify common types of graphs and their different uses • Identify features of tables, graphs and charts • Locate specific information • Perform calculations to interpret information • Explain how statistics can inform and persuade • Identify misleading statistical information	• Oral • Written • Practical test • Observation	

	• Discuss information relevant to the workplace		
6. Collect data and construct routine tables and graphs for work	• Identify features of common tables and graphs • Identify uses of **different tables and graphs** • Determine data and variables to be collected • Determine audience • Select a method to collect data • Collect data • Collate information in a table • Determine suitable scale and axes • Draft and draw graph to present information • Check that data meets the expected results and context • Report or discuss information using formal and informal mathematical language	• Written • Practical test • Observation	
7. Use basic functions of calculator	• Identify and use keys for basic 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 • Make estimations to check reasonableness of problem solving process, outcome and its appropriateness to the context and task • Use formal and informal mathematical language and appropriate symbolism and conventions to communicate the result of the task	• Written • Practical test • Observation	

Suggested Methods of Instruction

- Demonstrations
- Role playing
- Viewing of related videos
- Discussion
- Assignments

Recommended resources

- Calculators
- Basic measuring instruments

DIGITAL LITERACY

UNIT CODE: SEC/CU/CS/BC/3/5/A

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

Duration of Unit: 45 hours

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

Summary of Learning Outcomes
1. Identify computer software and hardware
2. Apply security measures to data, hardware, software in automated environment
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 • Laws governing protection of ICT	• Written tests • Oral presentation • Observation • Project
3. Apply computer software in solving tasks	• Operating system • Word processing • Spread sheets	• Oral questioning • Observation • Project

	• Data base design and manipulation • Data manipulation, storage and retrieval	
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 Instruction
- Demonstration
- Viewing of related videos
- Discussions
- Assignments
- Direct instructions

Recommended Resources
- Computers
- Other digital devices
- Printers
- Storage devices
- Internet access

- Computer software

ENTREPRENEURIAL SKILLS

UNIT CODE: SEC/CU/CS/BC/04/5/A

Relationship to Occupational Standards

This unit addresses the Unit of Competency: Demonstrate Entrepreneurship

Duration of unit: 70 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 an entrepreneur
2. Demonstrate knowledge of entrepreneurship and self-employment
3. Identify entrepreneurship opportunities
4. Create entrepreneurial awareness
5. Apply entrepreneurial motivation
6. Develop innovative business 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	• 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/05/5/A

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

Duration of Unit: 50 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 workplace ethics.

Summary of Learning Outcomes
1. Conduct self-management
2. Demonstrate interpersonal communication
3. Demonstrate critical safe work habits
4. Lead small teams
5. Plan and organize work
6. Maintain professional growth and development
7. Demonstrate workplace learning
8. Demonstrate problem solving skills
9. Demonstrate workplace ethics

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 ❑ Emotional intelligence ❑ Assertiveness versus aggressiveness ❑ Expressing personal thoughts, feelings and beliefs ❑ Developing and maintaining high self-esteem ❑ Developing and maintaining	❑ Written tests ❑ Oral questioning ❑ Interviewing ❑ Portfolio of evidence ❑ Third party report

	positive self-image ❑ Articulating ideas and aspirations ❑ Accountability and responsibility ❑ Good work habits ❑ Self-awareness ❑ Self-development ❑ Financial literacy ❑ Healthy lifestyle practices	
2. Demonstrate interpersonal communication	❑ Meaning of interpersonal communication ❑ Listening skills ❑ Types of audience ❑ Writing skills ❑ Reading skills ❑ Meaning of empathy ❑ Understanding customers' needs ❑ Establishing communication networks ❑ Sharing information	❑ Written tests ❑ Oral questioning ❑ Interviewing ❑ Portfolio of evidence ❑ Third party report
3. Demonstrate critical safe work habits	❑ Stress and stress management ❑ Punctuality and time consciousness ❑ Leisure ❑ Integrating personal objectives into organizational objectives ❑ Resources utilization ❑ Setting work priorities ❑ HIV and AIDS ❑ Drug and substance abuse ❑ Handling emerging issues	❑ Written tests ❑ Oral questioning ❑ Interviewing ❑ Portfolio of evidence ❑ Third party report
4. Lead a small team	❑ Leadership qualities ❑ Team building ❑ Determination of team roles and objectives ❑ Team performance indicators ❑ Responsibilities in a team ❑ Forms of communication ❑ Complementing team activities ❑ Gender and gender mainstreaming ❑ Human rights ❑ Maintaining relationships ❑ Conflicts and conflict resolution	❑ Written tests ❑ Oral questioning ❑ Interviewing ❑ Portfolio of evidence ❑ Third party report

	Core Competency	Required Knowledge	Assessment Methods

5.	Plan and organize work	❑ Functions of management
		  • Planning
		  • Organizing
		❑ Time management
		❑ Decision making process
		❑ Task allocation
		❑ Evaluating work activities
		❑ Resource utilization
		❑ Problem solving
		❑ Collecting and organising information
			❑ Written tests
			❑ Oral questioning
			❑ Interviewing
			❑ Portfolio of evidence
			❑ Third party report

6.	Maintain professional growth and development	❑ Opportunities for professional growth ❑ Assessing training needs ❑ Licenses and certifications for professional growth and development ❑ Pursuing personal and organizational goals ❑ Identifying work priorities ❑ Recognizing career advancement	❑ Written tests ❑ Oral questioning ❑ Interviewing ❑ Portfolio of evidence ❑ Third party report
7.	Demonstrate workplace learning	❑ Managing own learning ❑ Contributing to the learning community at the workplace ❑ Cultural aspects of work ❑ Variety of learning context ❑ Application of learning ❑ Safe use of technology ❑ Identifying opportunities ❑ Generating new ideas ❑ Workplace innovation ❑ Performance improvement ❑ Handling emerging issues ❑ Future trends and concerns in learning	❑ Written tests ❑ Oral questioning ❑ Interviewing ❑ Portfolio of evidence ❑ Third party report
8.	Demonstrate problem solving skills	❑ Problem identification ❑ Problem solving ❑ Application of problem-solving strategies ❑ Resolving customer concerns	❑ Written tests ❑ Oral questioning ❑ Interviewing ❑ Portfolio of evidence ❑ Third party report

9. Demonstrate workplace ethics	❑ Meaning of ethics ❑ Ethical perspectives ❑ Principles of ethics ❑ Values and beliefs ❑ 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
- ❑ Discussion
- ❑ Presentations
- ❑ Case studies
- ❑ 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/06/5/A

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

Duration of Unit: 25 hours

Unit Description
This unit describes the competencies required to demonstrate understanding of environmental literacy. It involves controlling environmental hazard, controlling control 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 and monitoring activities on environmental protection/programs.

Summary of Learning Outcomes
1. Control environmental hazards
2. Control environmental Pollution
3. Demonstrate sustainable use of resource
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

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Control environmental hazards	❑ Purposes and content of Environmental Management and Coordination Act 1999 ❑ Purposes and content of Solid Waste Act ❑ Storage methods for environmentally hazardous materials ❑ Disposal methods of hazardous wastes ❑ Types and uses of PPE in line with environmental regulations ❑ Occupational Safety and Health Standards (OSHS)	❑ Written test ❑ Oral questions ❑ Observation
2. Control environmental	❑ Types of pollution ❑ Environmental pollution control	❑ Written test ❑ Oral

		measures	questions
	Pollution control	❑ Types of solid wastes	❑ Observation
		❑ Procedures for solid waste management	
		❑ Different types of noise pollution	
		❑ Methods for minimizing noise pollution	
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 test ❑ Oral questions ❑ Observation
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 test ❑ Oral questions ❑ Observation
5.	Identify Environmental legislations/conventions for environmental concerns	❑ Environmental issues/concerns ❑ Environmental legislations /conventions and local ordinances ❑ Industrial standard /environmental practices ❑ International Environmental Protocols (Montreal, Kyoto) ❑ Features of an environmental strategy	❑ Written questions ❑ Oral questions ❑ Observation
6.	Implement specific environmental programs	❑ Community needs and expectations ❑ Resource availability ❑ 5 s of good housekeeping ❑ Identification of programs/Activities ❑ Setting of individual roles /responsibilities ❑ Resolving problems /constraints encountered ❑ Consultation with stakeholders	❑ Written questions ❑ Oral questions ❑ Observation

7. Monitor activities on Environmental protection/Programs	❏ Periodic monitoring and Evaluation of activities ❏ Gathering feedback from stakeholders ❏ Analysing 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 ❏ Observation

Suggested Methods of Instruction
- Instructor led facilitation of theory
- Demonstration by trainer
- Viewing of related videos
- Project
- Assignements
- Role play

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
- Ccompany environmental management systems (EMS)
- Montreal Protocol
- Kyoto Protocol

OCCUPATIONAL SAFETY AND HEALTH PRACTICES

UNIT CODE: SEC/CU/CS/BC/07/5/A

Relationship to Occupational Standards

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

Duration of Unit: 25 hours

Unit Description

This unit specifies the competencies required to identify workplace hazards and risk, identify and implement appropriate control measures and implement 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 is conducted by ❑ Authorized personnel or agency ❑ Gathering of OHS issues and/or concerns raised	❑ Oral questions ❑ Written tests ❑ Portfolio of evidence ❑ Third party report
2. Control OSH hazards	❑ Prevention and control measures, including use of PPE (personal protective equipment) for specific hazards are identified and implemented ❑ Appropriate risk controls based on result of OSH hazard evaluation is	❑ Oral questions ❑ Written tests ❑ Portfolio of evidence ❑ Third party report

	recommended	
	❑ Contingency measures, including emergency procedures during workplace incidents and emergencies are recognized and established in accordance with organization procedures	
3. Implement OSH programs	❑ Providing information to work team about company OHS program, procedures and policies/guidelines ❑ Participating in implementation of OSH procedures and policies/ guidelines ❑ Training of team members and advice on OSH standards and procedures ❑ Implementation of procedures for maintaining OSH-related records	❑ Oral questions ❑ Written tests ❑ Portfolio of 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/01/5/A

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

Duration of Unit: 60 hours

Unit Description
This unit covers the competencies required to effectively use digital devices such as smart phones, tablets, laptops and desktop PCs. It entails identifying 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
7. Identify computer software and hardware
8. Apply security measures to data, hardware and software
9. Apply computer software in solving tasks
10. Apply internet and email in communication at workplace
11. Apply desktop publishing in official assignments
12. Prepare presentation packages

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
7. 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
8. Apply security measures to data, hardware and software	• Data security and control • Security threats and control measures • Types of computer crimes	• Written tests • Oral presentation • Observation

	• Detection and protection against computer crimes • Laws governing protection of ICT	• Project
9. 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
10. 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
11. 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
12. 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

<p style="text-align: center">COMPUTER REPAIR AND MAINTENANCE</p>

UNIT CODE: SEC/CU/CS/CR/01/5/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 competeny 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
2. Dismantle faulty components	- Meaning of terms - Computer dismantling tools - Computer components and dismantling procedures - Handling of computer components - Safety precautions - Hardware - Software	- Written tests - Observation - Oral questioning - Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	• Personnel	

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 Instruction
- 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/02/5/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 of Cyber security laws, policies and regulations. It involves demonstrating the understanding of cyber security policies, laws and regulations, participating in developing cyber security policy, participating in implementing Cyber security policies and regulations, participating in evaluating Cyber security policies, complying with Cyber security policies and regulations and monitoring effectiveness of Cyber security policy in an organization.

Summary of Learning Outcomes

1. Demonstrate of cyber security policies, laws and regulations
2. Demonstrate understanding of different Cyber security policies and regulations
3. Participate in developing Cyber Security policy
4. Implement Cyber Security policy and regulations
5. Participate in evaluating Cyber security policy
6. Comply with Cyber security policy and regulations
7. 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. Participate in developing 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. Participate in evaluating 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. Comply with 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 • Cybercrime Act 2018
Materials and supplies • Stationery	**Tools** Framework

COMPUTER NETWORKING

UNIT CODE: SEC/CU/CS/CR/03/5/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. 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. Perform Network security
6. Document network report
7. Train network users
8. 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. Perform Network security	• Meaning of terms
	• Organization cyber security policy
	• Vulnerability assessment
	• Tools in network security e.g
	  • Antivirus
	  • Firewalls
		• Written tests
		• Oral questioning
		• Practical tests
		• Observation

6. Document network report	• Meaning of terms • Preparation of networking report • Report sharing • Report filing	• Written tests • Oral questioning • Practical tests • Observation
7. Train network users	• Meaning of terms • Identification and training of network users. • Preparation of network training manuals	• Written tests • Oral questioning • Practical tests • Observation
8. 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	

SOFTWARE APPLICATION SECURITY

UNIT CODE: SEC/CU/CU/CR/06/5/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 and preparing 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
	  • Environment
	  • Software and Hardware
		• Observation
		• Written tests
		• Oral questioning
		• Practical tests

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

Learning Outcome	Content	Suggested Assessment Methods
4 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	- Stationery

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

DATABASE SECURITY

UNIT CODE: SEC/CU/CS/CR/05/5/A

Relationship to Occupational Standards
This unit addresses the unit of competency: Provide 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 and threats in database	• Written tests • Oral questioning • Observation • Practical tests

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

	• Environment in installation of database patches		
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	• Written tests • Oral questioning • Observation • Practical tests	

	backups
	• Storage of database backups

Suggested Methods 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	

ADMINSTRATION OF CYBER SECURITY SYSTEM

UNIT CODE: SEC/CU/CU/CR/06/5/A

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

Duration of Unit: 130 hours

Unit Description

This unit covers the competencies required to administer Cyber security system. It involes identifying and analysing information to be protected, establishing systems to be administered, assessing system compatibility, monitoring system performance, documenting system administration report and establishing a Cyber security backup and restoration plan.

Summary of Learning Outcomes

1. Identify and analyze information to be protected
2. Establish systems to be administered
3. Asses system's compatibility
4. Monitor system performance
5. Document system administration report
6. Establish a cyber-security back up and restoration plan

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 • Technology in information storage and analysis • Information access control • Information analysis	• Observation • Written tests • Oral questioning • Practical tests
2. Establish systems to be administered	• 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. Monitor system performance	• Meaning of terms • System monitoring process • System simulation • Logs auditing • Patch management	• Observation • Oral questioning • Practical tests • Written tests
5. Document system administration report	• Meaning of terms • Report preparation • Report dissemination • Report filing	• Observation • Written tests • Oral questioning • Practical tests

6. 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

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	

UNIT CODE: SEC/CU/CS/CR/7/5/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 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

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 resources	• Meaning of terms • User identification and log in credentials • Service, protocol ,workgroup and database enumeration	• Observation • Oral questioning • Practical tests • Written tests

Learning Outcome	Content	Suggested Assessment Methods
	• Password cracking	
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	