

MODULE 6

UNIT CATEGORY	ISCED UNIT CODE	TVET CDACC UNIT CODE	UNIT NAME	DURATION (HOURS)
CORE	0612 551 04A	IT/CU/ICTA/CR/02/6/MA	ICT Security Management	150
CORE	0613 551 05A	IT/CU/ICTA/CR/03/6/MA	Desktop Application	280
Sub-Total Hours				430
Industrial Training				480
Total Hours				1,060

ICT SECURITY

ISCED UNIT CODE: 0612 551 16A

TVET CDACC UNIT CODE: IT/CU/ICTA/CR/02/6/MA

Duration of Unit: 150 Hours

Relationship to Occupational Standards

This unit addresses the Unit of Competency: Manage ICT security.

Unit Description

This unit covers the competencies required to manage ICT security. It involves assessing security needs, installing security control measures and maintains ICT system security.

Summary of Learning Outcomes

Learning Outcomes	Duration (Hours)
1. Assess security needs	50
2. Install security control measures	70
3. Maintain ICT system security	30
Total Hours	150

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Assess the security needs	1.1. Documentation of ICT security assets 1.1.1. Introduction to ICT security 1.1.1.1. Definition of terms 1.1.1.2. Importance of securing ICT assets 1.1.1.3. Principles of information security 1.1.1.3.1. Confidentiality 1.1.1.3.2. Integrity 1.1.1.3.3. Availability 1.1.2. ICT security regulations, standards and policies 1.1.2.1. Computer misuse and cyber-crimes act, 2018 1.1.2.2. The data protection act 2019 1.1.2.3. Information security management systems standard (KS ISO/IEC 27001:2022) 1.1.3. ICT security assets 1.1.3.1. Software 1.1.3.2. Hardware 1.1.3.3. Data 1.1.3.4. Network 1.1.3.5. Physical 1.1.3.6. Policy 1.1.3.7. People	• Practical • Projects • Third Party Reports • Portfolio of evidence • Written tests

	1.1.4. Importance of assessing Security needs 1.1.5. ICT security Control Measures 1.1.5.1. Software 1.1.5.2. Hardware 1.1.5.3. Firmware 1.1.5.4. Data 1.2. ICT security threats 1.2.1. Types of ICT security threats 1.2.1.1. Malware 1.2.1.2. Virus 1.2.1.3. Phishing 1.2.1.4. Hacking 1.2.1.5. Denial of service 1.2.2. ICT security vulnerabilities 1.3. ICT security risk assessment 1.3.1. ICT security risk identification 1.3.2. Conducting ICT security risk assessment 1.3.3. ICT security risk prioritization 1.3.4. ICT security risk levels 1.3.5. Development of mitigation measures 1.4. ICT security risk assessment report 1.4.1. Importance of security risk assessment report 1.4.2. Components of ICT risk assessment report 1.4.3. Compilation of ICT risk assessment report	
--	--	--

2. Install security control measures	2.1 Physical control measures 2.1.1 Introduction to security control measures 2.1.2 Implementation of Physical control measures 2.1.2.1 Grills 2.1.2.2 Security guards 2.1.2.3 Firewall 2.1.2.4 Locks 2.1.2.5 Burglar proofing 2.1.2.6 Security alarms 2.1.2.7 CCTV 2.2 Logical security control measures 2.2.1 Implementation of logical control measures 2.2.1.1 Firewall 2.2.1.2 Encryption 2.2.1.3 Authentication 2.2.1.4 Authorization 2.2.1.5 Accounting 2.2.1.6 Remote storage 2.2.1.7 Anti – malware 2.2.1.8 Update/Patches 2.3 Testing the implemented ICT security control measures 2.3.1 Types of testing techniques 2.3.2 Testing tools	• Practical • Projects • Third Party Reports • Portfolio of evidence • Written tests
3. Maintain ICT system security	3.1 Introduction to ICT security monitoring 3.1.1 Importance of monitoring ICT system security 3.1.2 ICT security monitoring tools 3.2 ICT security system monitoring report	• Practical • Projects • Third Party Reports • Portfolio of evidence

	3.2.1 Importance of ICT system security monitoring report 3.2.2 Preparation of ICT system security monitoring report 3.3 Updating ICT security system	Written tests
--	---	---

Suggested Methods of Delivery

- Presentations and practical demonstrations by trainer;
- Guided learner activities and research to develop underpinning knowledge;
- Supervised activities and projects in a workshop;
- The delivery may also be supplemented and enhanced by the following, if the opportunity allows:
 - Visiting lecturer/trainer from the ICT sector;
 - Industrial visits.

Recommended Resources for 25 trainees

S/No.	Category/Item	Description/Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	Learning Materials			
1.	Textbooks		5 pcs	5:1
2.	Installation manuals			
3.	Charts			
4.	PowerPoint presentations	For trainer's use		
B	Learning Facilities & infrastructure			
5.	Lecture/theory room		1	25:1

6.	Computer Laboratory		1	25:1
C	Consumable materials			
7.	Printing papers		1 ream	1:20
8.	Toners		2 pcs	13:1
9.	Assorted colour of whiteboard markers			
D	Tools and Equipment			
10.	Computers		25 pcs	1:1
11.	Password management software		25 pcs	1:1
12.	25-seat license Monitoring tools		25 pcs	1:1
13.	CCTV Cameras		5 pcs	5:1
14.	DVR/NVR Machine		1 Pc	25:1
15.	External DVR Hard disk		1 pc	25:1
16.	CCTV Monitor (24 inch)		1 pc	25:1
17.	25-seat license Antivirus			1:1