CONTROL ICT SECURITY THREATS

UNIT CODE: IT/OS/ICT/CR/3/6

UNIT DESCRIPTION

This unit covers the competencies required to provide ICT security. They include identification of security threats, installation of security control measures, implementation of security measures, testing of system vulnerability and monitoring of the security system.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT	**PERFORMANCE CRITERIA** ***(Bold and italicised terms are elaborated in the Range)***
1. Identify security threats	1.1 ***Security threats*** are identified based on the vulnerability of the system. 1.2 Security threats are categorised according to the risk impact 1.3 Appropriate Security measures are selected as per the Security threats
2. Establish and Install security control measures	2.1 ICT Security policy is implemented as per the ***Kenya security act 2018*** 2.2 ***Security control measures*** are identified and categorized as per the laws governing security in ICT. 2.3 Evaluation of Security control measures is done as per the ICT Security policy 2.4 Installation of Security control measures is done as per the ICT security policy
3. Deploy Security Measures	3.1 Physical control measures are implemented according to the ICT security policy. 3.2 Logical security control measures are implemented according to the ICT security policy. 3.3 ***ICT Security policy*** is implemented According to the Kenya security Act 2018.
4. Test system vulnerability	4.1 Schedule system testing plan is developed 4.2 Vulnerable levels of the system are identified. 4.3 Security ***ethical penetration*** is done as per the ICT security policy. 4.4 Report on system vulnerability is generated

ELEMENT	PERFORMANCE CRITERIA ***(Bold and italicised terms are elaborated in the Range)***
	4.5 Corrective action is taken based on the System Vulnerability report
5. Monitor security system	5.1 Performance of the security systems is evaluated. 5.2 Reports on security system are generated 5.3 Security systems are updated or overhauled based on the security system report.

RANGE

Variable	**Range** ***May include but is not limited to:***
1. Security threats	1.1 Malicious hackers 1.2 Industrial espionage 1.3 Employee sabotage 1.4 Fraud and theft 1.5 Loss of physical and infrastructure support 1.6 Errors and Omissions
2. Security control measures	2.1 Preventive 2.2 Detective 2.3 Responsive
3. ICT Security policy	3.1 refers to a document that has a set of rules enacted by an organization to ensure that all users or networks of the IT structure within the organization's domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organization stretches its authority.
4. Ethical Penetration	4.1 refers to legally breaking into computers and devices to test an organization's defences.

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

1. Security risk management techniques and procedures
2. Types of security threats and their control measures
3. Security audit procedures
4. ICT security policy
5. Strategies for Mitigating risks
6. Categories of Security threats
7. Penetration testing skills

FOUNDATION SKILLS

The individual needs to demonstrate the following foundation skills:	
• Communications (verbal and written); • Time management; • Penetration Skills • Problem solving; • Planning;	• Decision making; • Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Identified and classified security threats 1.2 Identified and categorized security control measures 1.3 Implemented ICT security policy 1.4 Developed a schedule system testing plan
2. Resource Implications	Resources the same as that of workplace are advised to be applied including 2.1 Computers 2.2 Servers 2.3 Data centres 2.4 Security software
3. Methods of Assessment	Competency may be assessed through: 3.1 Observation 3.2 Oral questioning 3.3 Practical test in conducting test 3.4 Demonstration of interpretation of test results
4. Context of Assessment	Competency may be assessed individually 4.1 In the actual workplace 4.2 Simulated environment of the work place
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.