

MONITOR COMPUTER NETWORK SECURITY

ISCED UNIT CODE: 0612 451 09A

TVET CDACC UNIT CODE: IT/OS/NSA/CR/06/5/MA

UNIT DESCRIPTION

This unit covers the competencies required to Monitor Computer network security. It involves the following: Conduct computer network security assessment, Monitor Computer Network Firewall activities and perform fundamental Computer Network segmentation

Elements <i>These describe the key outcomes which make up workplace functions</i>	Performance Criteria <i>These are assessable statements which specify the required level of performance for each of the elements</i> <i>(Bold and italicized terms are elaborated in the range)</i>
1. Conduct computer network security assessment	1.1 <i>Network Security Threats & Vulnerabilities</i> are identified and prioritized as per work procedure. 1.2 <i>Network Security Controls</i> are implemented as per work procedure. 1.3 Network Risk Assessment Report is documented as per work procedure
2 Monitor Computer Network Firewall activities	2.1 <i>Firewall activities</i> are monitored as per work procedures 2.2 Firewall updates are performed as per work procedures 2.3 Computer network traffic is monitored as per work procedure
3. Perform fundamental Computer Network segmentation	3.1 <i>IP addressing scheme</i> is performed as per industry standards. 3.1 <i>Network segmentation</i> is determined as per the network design. 3.3 <i>Network privileges</i> are allocated according to the network configuration

RANGE

This section provides work environments and conditions to which the performance criteria apply. It allows for different work environments and situations that will affect performance.

1. Network security Threats & Vulnerabilities may include but not limited to;	● Malware ● Phishing ● Man in the middle attack ● Denial of service attack ● SQL injection ● Weak authentication and authorization ● Physical security threats
2. Network Security Controls may include but not limited to;	● Firewalls ● Network segmentation ● Network monitoring and logging ● Authentication mechanisms
3. Firewall activities may include but not limited to;	● Packet filtering ● Logging and reporting ● Bandwidth management ● URL Filtering
4. IP addressing scheme may include but not limited to;	● Classful addressing ● Private IP addressing ● Public IP addressing
5. Network segmentation may include but not limited to;	● VLANs ● Subnetting ● Firewalls ● Physical segmentation
6. Network privileges may include but not limited to;	● Administrator privileges ● User privileges ● Read-only access ● Remote access privileges

REQUIRED KNOWLEDGE AND SKILLS

This section describes the knowledge and skills required for this unit of competency.:

Required knowledge

- Network architecture
- Network components and devices
- Network security measures
- Network monitoring procedures
- Network testing procedures
- Understanding operating system
- Safety awareness
- Environmental conservation
- Workplace safety and health

Required skills

- Computer Literacy
- Critical thinking
- Communication skills
- Problem-solving skills
- Analytical skills
- Creativity and innovation
- Network testing techniques
- Network security configuration
- Network configuration techniques
- Network Monitoring
- Technical proficiency
- Project management
- Operating systems proficiency

EVIDENCE GUIDE

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

1 Critical aspects of competency	Assessment requires evidence that the candidate: 1.1 Conducted computer network security assessment as per work procedure 1.2 Monitored network firewall activities as per work procedure 1.3 Performed fundamental Network Segmentation
2 Resource implications	The following resources should be provided: 2.1 Appropriately simulated environment where assessment can take place 2.2 Access to relevant work environment 2.3 Resources relevant to the proposed activities or tasks; including computers, media, routers, switches, ports etc
3 Methods of assessment	Competency in this unit may be assessed through: 3.1 Observation 3.2 Oral questioning 3.3 Portfolio of evidence 3.4 Interviews 3.5 Third party report 3.6 Practical assessment 3.7 Written tests

4 Context of assessment	4.1 This Competency may be assessed in a workplace or a simulated workplace
5 Guidance information for assessment	5.1 Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.