

CONFIGURE COMPUTER NETWORK SECURITY

ISCED UNIT CODE: 0612 551 06A

TVET CDACC UNIT CODE: IT/OS/NSA/CC/04/5/MA

UNIT DESCRIPTION

This unit covers the competencies required to Configure Computer network security. It involves conducting computer network risk assessment, performing computer network segmentation, configuring network firewall and conducting Computer Network security user training.

Elements These describe the key outcomes which make up workplace functions	Performance Criteria These are assessable statements which specify the required level of performance for each of the elements <i>(Bold and italicized terms are elaborated in the range)</i>
1. Conduct computer network risk assessment	1.1 Inventory of network components is taken as per work procedure 1.2 <i>Security Threats & Vulnerabilities</i> are identified and prioritized as per work procedure. 1.3 <i>Security Controls</i> are developed and implemented as per work procedure. 1.4 Risk Assessment Report is documented as per work procedure.
2. Perform computer network segmentation	2.1 IP addressing scheme is performed as per IEEE 802.3 and IEEE 802.11. 2.2 Network segmentation is determined as per the network design 2.3 Network privileges are allocated according to the network configuration.
3. Configure computer network firewall	3.1 <i>Firewall</i> is secured as per work procedure 3.2 <i>Firewall</i> zones and an IP address structure are established as per work procedure 3.3 Access control lists are configured as per work procedure 3.4 Login and firewall services are configured as per work procedure 3.5 <i>Firewall</i> configuration is tested as per work policy 3.6 <i>Firewall</i> is periodically Managed as per Work procedure

4. Conduct Computer Network security user training	4.1 Security awareness training is conducted as per work procedure 4.2. Network security practices are implemented as per work procedure 4.3. Incident response training is conducted as per work procedure 4.4 Regular updates and refresher training is performed as per work procedure 4.5. Compliance training is conducted as per work procedure 4.6. Testing and simulation is performed as per work procedure.
--	--

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. Security threats and vulnerabilities may include but not limited to:	• Malware • Phishing • Denial of service • Man in the middle attack
2. Security Controls may include but not limited to:	• Preventive • Detective controls • Corrective controls • Deterrent controls • Compensating controls
3. Firewall may include but not limited to:	• Hardware firewall • Software firewall • Cloud firewall • Open source firewall

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
- Storage solutions
- 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.

Critical aspects of competency	Assessment requires evidence that the candidate: 1.1 Conducted computer network risk assessment as per work procedure 1.2 Performed computer network segmentation as per work procedure 1.3 Configured network firewall as per work procedure 1.4 Conducted computer network security user training as per work procedure
--------------------------------	---

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
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
Context of assessment	This Competency may be assessed: 4.1 in a workplace 4.2 in a simulated workplace
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.