BUILD SECURE NETWORK

UNIT CODE: SEC/OS/CS/CR/04/6/A

UNIT DESCRIPTION

This unit covers the competencies required in building secure network. It involves confirming user requirements and network equipment, reviewing security issues, analyzing network security protocols and features, designing and perimeters, installing and configuring perimeter solutions, configuring internal network devices, testing and verifying design performance and preparing network report.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements ***(Bold and italicised terms are elaborated in the Range)***
1. Confirm user requirements and network equipment	1.1 Network use is identified as per the organizations ICT policy and industry best practices 1.2 Equipment and network topology are established in line with workplace procedures 1.3 Network speed is established as per its source 1.4 Number of network users are determined in line with organization requirement 1.5 Perimeter type is identified as per the organization requirements 1.6 Security perimeters is established from the organization's objectives
2. Review security issues	2.1 Security threats in the organization are identified as per the its set up 2.2 Security issues are reviewed as per the industry best practices 2.3 Security control measures in the organization are identified in line with the ICT policy
3. Analyse network security protocols and features	3.1 Types of network security protocols are identified as per the industry best practice 3.2 Application of network security protocols are established in line with the industry best practice 3.3 Required network security protocols are established as per the client's requirements
4. Plan and design perimeter solution	4.1 Perimeter solution is designed as per the expected use and industry best practices 4.2 Perimeter schedule is designed in line with the organization ICT policy

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements ***(Bold and italicised terms are elaborated in the Range)***
	4.3 Perimeter design is approved as per the clients requirements 4.4 Perimeter design is tested for its functionality as per the expected objectives
5. Install and configure perimeter solutions	5.1 Perimeter solution system is acquired in line with the design 5.2 System is installed as per the design and the organization ICT policy 5.3 System is configured as per the manufacturers guidelines 5.4 Perimeter solution installed is tested as per the organization ICT policy 5.5 Parameters to be configured are identified as per the design
6. Configure internal network devices	6.1 Devices to be configured are identified from the system design 6.2 Internal devices compatibility are compared with the designed system 6.3 Internal network devices are configured as per manufacturers guidelines 6.4 Network devices are integrated to the security perimeter as per the organization ICT policy
7. Test and verify design performance	7.1 Types of tests are identified as per the systems efficiency 7.2 System performance test is conducted according to workplace procedures 7.3 Errors are checked and debugged as per the design 7.4 Threats are simulated in performance verification as per the work place procedures 7.5 Continuous monitoring of security perimeter performance is conducted as per the organization policy
8. Prepare network report	8.1 Network reports are prepared in line with the organizations approved format 8.2 Network reports are shared with relevant parties as per the organization policy 8.3 Network reports are documented and filled according organization filing system

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements ***(Bold and italicised terms are elaborated in the Range)***
	8.4 Network design recommendations are prepared and shared with the relevant parties

RANGE

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

Variable	Range
1. ICT components and infrastructure may include but not limited to:	• Software • Hardware • People • Data • Procedures • Information

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Troubleshooting techniques
- ICT Infrastructure auditing procedures
- ICT safety and precautious measures
- ICT Prevention measures
- Performance monitoring techniques
- ICT policy
- Causes of hardware and software failure
- Components of ICT Infrastructure
- User training procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:

• Communications (verbal and written); • Proficient in ICT; • Time management; • Analytical • 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 perimeter type as per the organization requirements 1.2 Identified security threats in the organization as per its set up 1.3 Identified security control measures in the organization in line with the ICT policy 1.4 Types of network security protocols are identified as per the industry best practice 1.5 Designed perimeter solution with self-defensive mechanism 1.6 Tested perimeter design functionality as per the organization objectives 1.7 Configured the system as per the manufacturers guidelines 1.8 Installed perimeter solution was tested as per the organization ICT policy 1.9 Configured internal network devices as per manufacturers guidelines 1.10 Integrated network devices to the security perimeter as per the organization ICT policy
2. Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Oral questioning 3.2 Practical demonstration 3.3 Observation
4. Context of	Competency may be assessed individually in the actual

Assessment	workplace or through simulated work environment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.