PERFORM COMPUTER REPAIR AND MAINTENANCE

UNIT CODE: SEC/OS/CS/CR/01/6/A

UNIT DESCRIPTION

This unit covers the competencies required to perform computer repair and maintenance. It involves performing troubleshooting, dismantling faulty components, repairing/replacing faulty components, upgrading computer software/hardware, and preparing and documenting maintenance reports.

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. Perform troubleshooting	1.1 Performance issues in the machine are identified as per the workplace procedures 1.2 ***Hardware and software are*** diagnosed in line with the standard operating procedure 1.3 Testing and troubleshooting tools are established as pert the industry best practices
2. Dismantle faulty components	2.1 Components to be dismantled are identified 2.2 Components are dismantled in line with the manufacturer's manuals 2.3 Dismantling tools and components are established in standard operating procedures 2.4 Component handling is aligned to the standard operating procedures
3. Repair/Replace faulty components	3.1 Diagnostic tools and instruments are identified as per the workplace policy 3.2 Components functionality is tested as per the manufacturer's manuals 3.3 Test parameters are compared with the expected output in line with the manufacturer's manuals 3.4 Faulty components are identified and removed as per the standard operating procedure 3.5 Faulty components are repaired/replaced in line with manufacturers manuals 3.6 Repaired/replaced components are tested for their functionality according to standard operating procedure

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)***
	3.7 Components are reassembled, and continuous monitoring performed as per the industries best practice
4. Upgrade computer hardware/software	4.1 Tools in managing software updates are established as per the industry best practice 4.2 Test environment is developed for hardware and software as per industry best practices 4.3 Licensed software and hardware are used in computer upgrades as per the organizations ICT policy 4.4 Schedule updates in lines with the organization policy 4.5 Upgraded computer hardware and software are tested in line with the organization policy
5. Prepare and document maintenance report	5.1 Maintenance report is prepared in line with the organizations approved format 5.2 Maintenance report is shared with the relevant parties 5.3 Prepared report is filed as per the organizations policy

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. Hardware may include but not limited to:	• Desktops • Central process unit (CPU) • Laptops • Mobile phones • Server boxes • Hard drives • Routers • Switches
2. Software may include but not limited to:	• Preventive • Detective

Variable	Range
	• Responsive

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Security risk management techniques and procedures
- Types of security threats and their control measures
- Security audit procedures
- ICT security policy
- Strategies for Mitigating risks
- Categories of Security threats
- 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 Diagnosed software and hardware in line with the standard operating procedure 1.2 Dismantled components in line with the manufacture's manuals 1.3 Tested components functionality as per the manufacturer's manuals 1.4 Tested repaired/replaced components functionality according to standard operating procedure 1.5 Monitoring reassembled components as per the industries best practice 1.6 Test environment was developed for hardware and software as per industry best practices 1.7 Prepared maintenance report in line with organizations

	approved format 1.8 Tested upgraded computer hardware and software were tested in line with the organization policy 1.9 Security threats were identified and classified as per the organization ICT policy 1.10 Security control measures were identified and categorized
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 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.