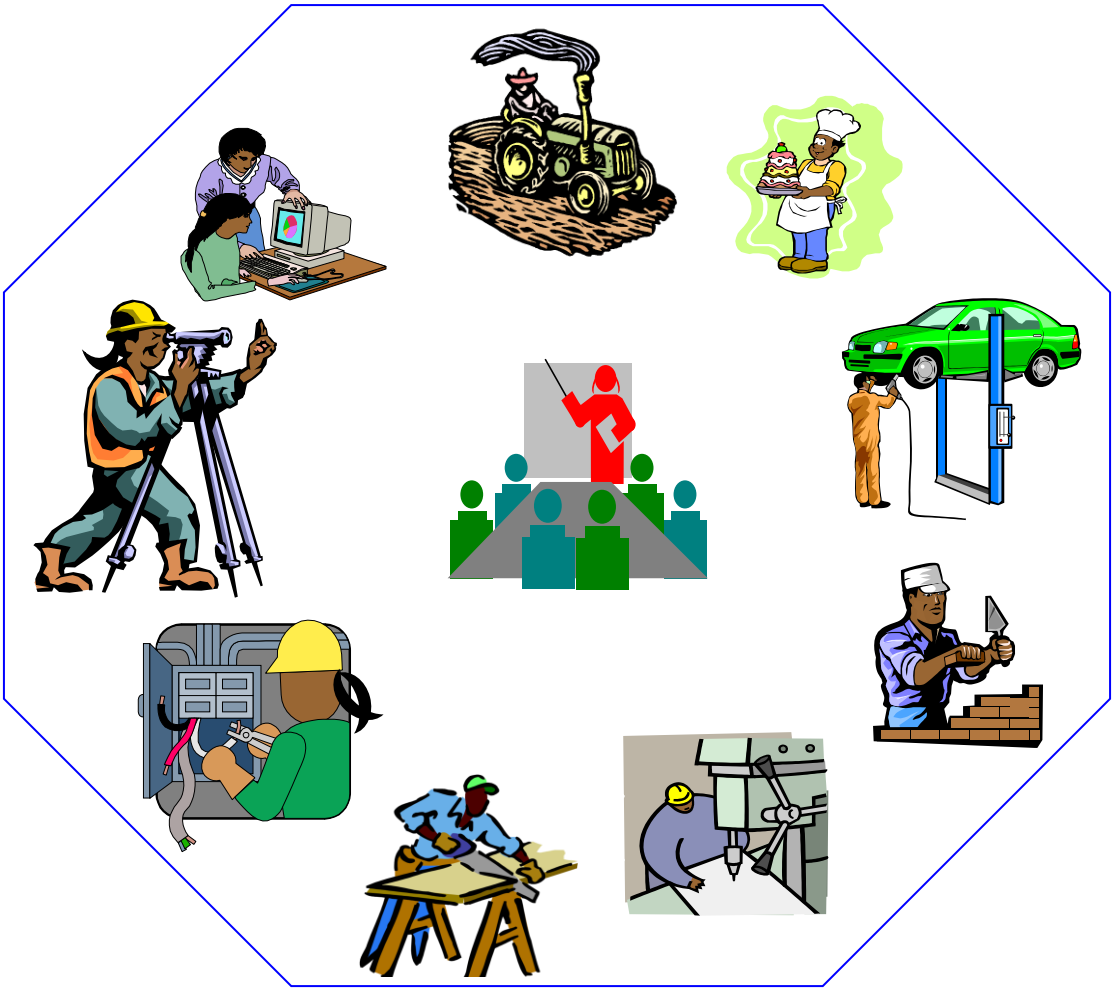
Federal Democratic Republic of Ethiopia

OCCUPATIONAL STANDARD

HARDWARE AND NETWORK SERVICING

NTQF Level I-V



Ministry of Education

Dec. 2021

Introduction

Ethiopia has embarked on a process of reforming its TVET-System. Within the policies and strategies of the Ethiopian Government, technology transformation – by using international standards and international best practices as the basis, and, adopting, adapting and verifying them in the Ethiopian context – is a pivotal element. TVET is given an important role with regard to technology transfer. The new paradigm in the outcome-based TVET system is the orientation at the current and anticipated future demand of the economy and the labor market.

The Ethiopia Occupational Standards (EOS) is the core element of the Ethiopian National TVET-Strategy and an important factor within the context of the National TVET-Qualification Framework (NTQF). They are national Ethiopia standards, which define the occupational requirements and expected outcome related to a specific occupation without taking TVET delivery into account.

This document details the mandatory format, sequencing, wording and layout for the Ethiopia Occupational Standard which comprised of Units of Competence.

A Unit of Competence describes a distinct work activity. It is documented in a standard format that comprises:

- Occupational title and NTQF level
- Unit code
- Unit title
- Unit descriptor
- Elements and Performance criteria
- Variables and Range statement
- Evidence guides

Together all the parts of a Unit of Competence guide the assessor in determining whether the candidate is competent.

The ensuing sections of this EOS document comprise a description of the respective occupation with all the key components of a Unit of Competence:

- chart with an overview of all Units of Competence for the respective level including the Unit Codes and the Unit Titles
- contents of each Unit of Competence (competence standard)
- occupational map providing the technical and vocational education and training (TVET) providers with information and important requirements to consider when designing training programs for this standard and for the individual, a career path

Occupational Standard: Hardware and Network Servicing

Occupational Code: EIS HNS

NTQF Level V

EIS HNS5 01 1221
Research and Review Hardware Technology Options for Organizations

EIS HNS5 02 1221
Prepare Disaster Recovery and Contingency Plan

EIS HNS5 03 1221
Assist with Policy Development for Client Support

EIS HNS5 04 1221
Establish and Maintain Client User Liaison

EIS HNS5 05 1221
Match IT Needs with the Strategic Direction of the Enterprise

EIS HNS5 06 1221
Install, Configure and Test Router

EIS HNS5 07 1221
Install and manage complex ICT networks

EIS HNS5 08 1221
Plan and Monitor the System Pilot

Occupational Standard: Hardware and Network Servicing

Occupational Code: EIS HNS

NTQF Level IV

EIS HNS4 01 1221
Provide Network System Administration

EIS HNS4 02 1221
Develop System Infrastructure Design Plan

EIS HNS4 03 1221
Build Internet Infrastructure

EIS HNS4 04 1221
Build a small wireless LAN

EIS HNS4 05 1221
Manage network security

EIS HNS4 06 1221
Determine Maintenance Strategy

EIS HNS4 07 1221
Conduct / Facilitate User Training

Occupational Standard: Hardware and Network Servicing

Occupational Code: EIS HNS

NTQF Level III

EIS HNS3 01 1221
Determine Best-Fit Topology

EIS HNS3 02 1221
Install and Manage Network Protocols

EIS HNS3 03 1221
Configure and Administer Server

EIS HNS3 04 1221
Monitor and Administer System and Network Security

EIS HNS3 05 1221
Identify and Resolve Network Problems

EIS HNS3 06 1221
Provide First Level Remote Help Desk Support

EIS HNS3 07 1221
Create Technical Documentation

`

Occupational Standard: Hardware and Network Servicing

Occupational Code: EIS HNS

NTQF Level II

EIS HNS2 01 1221
Operate Database Application

EIS HNS2 02 1221
Install and Optimise Operating System Software

EIS HNS2 03 1221
Administrate Network and Hardware Peripherals

EIS HNS2 04 1221
Implement Maintenance Procedures

EIS HNS2 05 1221
Maintain Equipment and Consumables

EIS HNS2 06 1221
Connect Internal Hardware components

EIS HNS2 07 1221
Apply Problem Solving Techniques to Routine Malfunction

EIS HNS2 08 1221
Care for Network and Computer Hardware

EIS HNS2 09 1221
Update and Document Operational Procedures

EIS HNS2 10 1221
Record Client Support Requirements

EIS HNS2 11 1221
Prevent and Eliminate MUDA

Occupational Standard: Hardware and Network Servicing

Occupational Code: EIS HNS

NTQF Level I

EIS HNS1 01 1221
Connect Hardware Peripherals

EIS HNS1 02 1221
Operate Personal Computer

EIS HNS1 03 1221
Protect Application or System Software

EIS HNS1 04 1221
Install Software Application

EIS HNS1 05 1221
Develop Computer Keyboard Skill

EIS HNS1 06 1221
Create and Use Spreadsheet

EIS HNS1 07 1221
Maintain Equipment and Software Inventory and Documentation

EIS HNS1 08 1221
Identify and Use Network Hand Tools

EIS HNS1 09 1221
Access and Use Internet

EIS HNS1 10 1221
Apply 5S Procedures

NQTF Level V

TOP

Occupational Standard: Hardware and Network Servicing Level V	
Unit Title	**Research and Review Hardware Technology Options for Organizations**
Unit Code	**EIS HNS5 01 1221**
Unit Descriptor	This unit defines the competency required to apply research skills in conjunction with reviewing hardware solutions, as part of an analysis of emerging technology.

Elements	Performance Criteria
1. Research vendors, suppliers and IT industry specialists	1.1 Organizational needs and selection criteria is established 1.2 Suitable suppliers and vendors are determined. 1.3 Source information from suppliers and vendors
2. Evaluate and report on options	2.1 ***Hardware*** *is* reviewed and tested against organizational requirements. 2.2 Findings are report to ***appropriate person*** according to their suitability for organizational requirements 2.3 Information in a report is documented and submitted to appropriate person.

Variable	Range
Hardware	May include but not limited to: • Workstations • personal computers • modems And other connectivity devices • networks, • DSL modems • remote sites and • servers
Appropriate person	May include but not limited to: • supervisor • teacher • authorized business representative or client

Evidence Guide	
Critical Aspects of Competence	Demonstrates skills and knowledge in: • the ability to apply technical knowledge in the preliminary analysis of emerging technology according to organizational requirements or practices • Ability to convey and access conceptual information regarding emerging technology in relation to organizational needs.
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • Current industry and technology information sources (e.g. vendor seminars, expert email groups, etc, as mentioned above) • Current business practices in relation to preparing reports • Components of the business planning process relevant to the development of IT business solutions • Current industry-accepted hardware and software products, including broad knowledge of general features and capabilities, with particular reference to emerging trends and product design • Broad knowledge of vendor product directions such as self-configuring ADSL or cable modem-router-switch for the Small Office Home Office (SOHO) market • General knowledge of the client business needs, with a view to expanding into new possibilities, as presented by new technology • Basic knowledge of quality assurance practices, to promote reliable investigation processes • Basic knowledge of information gathering techniques • Industry networks • Key individuals and organizations within the IT industry
Underpinning Skills	Demonstrates skills to: • Solving unknown problems in a range of contexts, particularly in developing new approaches with new technology (this includes problem solving skills for resolving unpredictable problems, with reference to the new technology) • Basic planning skills in relation to scope, time, cost, quality, communications and risk management • Participating in the development of reports and summary findings Plain English literacy and communication skills in relation to analysis, evaluation and presentation of information, such as when presenting the results of testing

	new technology and proposing new potential directions as a result of this • Teamwork skills, involving the contribution to solutions and goals of a non-routine or developmental process, such as investigating new technology for new roles in the workplace • Group facilitation and presentation skills in relation to transferring and collecting information and gaining consensus on concepts and new proposals • Communication skills to convey complex and abstract concepts and information
Resources Implication	To demonstrate competency in this unit the learner will require access to: • Internet • Journals of industry/professional associations
Methods of Assessment	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level V	
Unit Title	**Prepare Disaster Recovery and Contingency Plan**
Unit Code	EIS HNS5 02 1221
Unit Descriptor	This unit defines the competency required to analyse the impact of the system on the organisation and carry out risk analysis, disaster recovery and contingency planning for the project.

Elements	Performance Criteria
1. Evaluate impact of system on business continuity	1.1 ***Business-critical functions*** and the security environment is Identify from documentation and from discussion with business area and ***project team***. 1.2 Critical data and ***software*** is identified from ***documentation*** 1.3 Potential impacts of business risk and ***threats*** on IT ***systems*** are assessed. 1.4 ***Statutory requirements***, commercial requirements and contingency possibilities are Identified and evaluated according to specifications and cost constraints
2. Evaluate threats to system	2.1 Threats to the system are identified with consideration of security analysis and internal and external business environment. 2.2 Risk minimisation alternatives are evaluated against specifications and cost constraints.
3. Formulate prevention and recovery strategy	3.1 Prevention and recovery options are evaluated to support critical business functions against business specifications and cost constraints 3.2 Current operational procedures are reviewed to ensure adequate risk safeguards and ***contingency plan*** are in place 3.3 Disaster recovery and prevention strategy is submitted to appropriate person for approval

4. Develop disaster recovery plan to support strategy	4.1 Resources required for disaster recovery are identified and documented according to specifications and cost constraints 4.2 Processes required for disaster strategy are identified and documented according to project standards 4.3 ***Cut-over criteria*** are identified before initiating disaster plan. 4.4 Disaster recovery plan is documented and submit to appropriate person for review and sign-off.

Variable	**Range**
Business-critical functions	May include but are not limited to • financial systems • customer service functions • payroll
Documentation	May follow • ISO/IEC/AS standards • audit trails • naming standards • version control • project management templates and report writing • maintaining equipment inventory • client training and satisfaction reports
Project team	May include: • Solution developers and business clients working together • Individual business analysts • A number of third-party solution developers working together • A number of different businesses working in partnership
Software	May include but is not limited to • commercial • in-house • packaged or customised software
Specifications	May include but is not limited to • technical requirements • user problem statement • current system functionality
Constraints	May include but is not limited to • time • budget • resource • hardware, software • policy and legal constraints
System	May include but is not limited to • databases • applications

	• servers • operating systems • gateways • application service provider and ISP
Appropriate person	May include a • supervisor • teacher • authorised business representative or client
Threats	May include: • Weather (storms, earthquake) • Security • Information technology failure (hardware, software) • Accident • Espionage • Sabotage (hackers) • Telecommunications network failure • Denial of service • Virus attack Supplementary questioning of the client may be used during the assessment phase, where necessary, to ensure that all issues relating to threats to the system are considered and appropriate choices made given the need to prevent, limit, recover, respond and recover from disasters
Back-up strategy	May include • hot standby site • warm standby site • cold standby site • mobile van • supplier • bureau • contacts through user group • third parties
Contingency plans	The contingency plan will vary in format and content detail, but will typically: • Identify weaknesses and provide for the implementation of a disaster prevention program • Minimise disruption to business operations • Provide a coordinated approach to the disaster recovery process
Statutory requirements	May include • legislation (e.g. Privacy Act) • industry-imposed controls and standards. In certain organisations (e.g. health and banking), there may be strict laws regarding confidentiality and reporting of data

Security environment	May Includes • legislation • organisational security policies • customs • expertise and knowledge that are, or may be, relevant The security environment also includes the threats to security that are, or are held to be, present in the environment
Cut-over criteria	May include: • Estimate of time before system is operational • Estimate of business impact • Authorisations to cut-over • Actual system down time • Refresher of cut-over plan
Commercial requirements	May include but not limited to: • Back-up • Storage and recovery of data • Access to internal network • Passwords/logons • Encryption • Firewalls • Hacking • Confidentiality • Integrity • Availability
Standards	May include • ISO/IEC/AS standards • organisational standards • project standards

Evidence Guide	
Critical Aspects of Competence	Demonstrates skills and knowledge in: • Evaluated impact of system on business continuity • Evaluated threats to system • Formulated prevention and recovery strategy • Developed disaster recovery plan to support strategy
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • Broad knowledge of basic engineering (e.g. when evaluating threats) • Broad knowledge of fire/safety knowledge (e.g. when formulating prevention and recovery strategy) • Detailed knowledge of back-up methodologies (e.g. when formulating prevention and recovery strategy) • Broad knowledge of systems engineering (e.g. when evaluating threats)

	• Specific components of the business planning process relevant to the development of IT business solutions (e.g. when evaluating impact of system on business continuity) • Broad knowledge of the client business domain (e.g. when evaluating impact of system on business continuity) • Detailed knowledge of the system's current functionality (e.g. when evaluating impact of system on business continuity)
Underpinning Skills	Demonstrates skills to: • Logistic management skills for identified resources and procedures skills (e.g. when IT hardware, software and resources required for disaster recovery are identified and documented according to project specifications and cost constraints) • Negotiation skills in relation to self and other team members and applied to a defined range of predictable problems (e.g. when business-critical functions are identified from project documentation and discussion with client business area and project team) • Project planning skills in relation to scope, time, cost, quality, communications, risk analysis and management (e.g. when business-critical functions are identified from project documentation and discussion with client business area and project team, and when contingency possibilities are identified and evaluated according to project specifications and cost constraints) • Research skills for specifying, analysing and evaluating broad features of a particular business domain and best practice in system development (e.g. when threats to the system are identified, taking into consideration security analysis and internal and external business environment) • Facilitation and presentation skills in relation to transferring and collecting information and gaining consensus on concepts (e.g. when business-critical functions are identified from project documentation and discussion with client business area and project team, and when disaster recovery plan is documented and submitted to higher authorities for review and sign-off
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices. • A vulnerability assessment and general definition of requirements • Business impact analysis • Acceptance test plan • Information technology security assurance specifications

Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level V	
Unit Title	**Assist with Policy Development for Client Support**
Unit Code	**EIS HNS5 03 1221**
Unit Descriptor	This unit defines the competence required to receive, review and carry out change requests, while utilizing a change management system according to client requirements.

Elements	**Performance Criteria**
1. Review change requests	1.1 Requests are received and documented for ***hardware*** and ***software*** changes, utilizing a change management system and according to organizational help desk procedures***.*** 1.2 ***System*** data are gathered and organized relevant to the change requests, using available diagnostic tools. 1.3 The proposed changes are reviewed against current and future business ***requirements.*** 1.4 System data are examined, with work team, in order to select appropriate changes to be carried out. 1.5 Selected changes are discussed and e clarified with ***client***.
2. Modify system according to requested changes	2.1 Potential solution is identified to solve problems***.*** 2.2 Recommendations about possible solutions are developed, documented, ranked and presented to the appropriate person for decision. 2.3 Implementation and evaluation of solutions are planned. 2.4 Recommended solutions are technically documented and submitted to appropriate person for confirmation.
3. Train on the use of modified system	3.1 Training is prepared to meet the needs of client in using the changed system. 3.2 Prepared training is delivered appropriately for client

	3.3 Evaluate the given training to confirm the expected result has been achieved

Variable	Range
Hardware	May include but not limited to: • workstations, personal computers, modems or other connectivity devices, networks, DSL modems, remote sites, servers
Software	May include but is not limited to commercial, in-house, packaged or customized software
System	May include but not limited to: • the hardware and software components that run a computer
Requirements	• May be in reference to the business, system, application, network or people in the organization
Client	May include but is not limited to internal departments, external organizations, individual people and employees
Organizational guidelines	May include but not limited to: • personal use of emails and internet access, content of emails, downloading information and accessing particular websites, opening mail with attachments, virus risk, dispute resolution, document procedures and templates, communication methods and financial control mechanisms.
Technical documentation	• May include but not limited to: • project specifications, reports, help references, technical manuals, training materials and self-paced tutorials, on-line help, user guides, brochures
Standards	May include but not limited to: • ISO/IEC/AS standards, organizational standards, project standards
Documentation	May follow ISO/IEC/AS standards, audit trails, naming standards, version control, project management templates and report writing, maintaining equipment inventory; client training and satisfaction reports
Occupational Health and Safety (OHS)	May include but not limited to: • correct posture, lighting, type of desk, type of monitor, style of chair, typing position, repetitive strain injury prevention, ventilation, light position, correct lifting method, and length of time in front of computer • May also include licensing-related and physical safety considerations such as general electrical safety and cabling, power supply and leads as they apply to computer and peripheral installations.

Evidence Guide	
Critical Aspects of Competence	A person must be able to demonstrate: • ability to identify daily work requirements and allocate work appropriately • ability to interpret financial documents in accordance with legal requirements
Underpinning Knowledge and Attitudes	• Federal and Regional Government legislative requirements affecting business operations, especially in regard to occupational health and safety (OHS), equal employment opportunity (EEO), industrial relations and anti-discrimination • technical or specialist skills relevant to the business operation • relevant industry code of practice • planning techniques to establish realistic timelines and priorities • identification of relevant performance measures • quality assurance principles and methods • relevant marketing, management, sales and financial concepts • methods for monitoring performance and implementing improvements • structured approaches to problem solving, idea management and time management
Underpinning Skills	• literacy skills to interpret legal requirements, company policies and procedures and immediate, day-to-day demands • communication skills including questioning, clarifying, reporting, and giving and receiving constructive feedback • numeracy skills for performance information, setting targets and interpreting financial documents and reports • technical and analytical skills to interpret business documents, reports and financial statements and projections • ability to relate to people from a range of social, cultural and ethnic backgrounds and physical and mental abilities • problem solving skills to develop contingency plans • using computers and software packages to record and manage data and to produce reports • evaluation skills for assessing work and outcomes • observation skills for identifying appropriate people, resources and to monitor work
Resource Implications	The following resources should be provided: • Access to relevant workplace documentation, financial records, and equipment
Methods of Assessment	Competence may be assessed through: • Interview / Written exam • Observation/Demonstration with Oral questioning
Context for Assessment	Competence may be assessed in the workplace or in a simulated work environment

TOP

Occupational Standard: **Hardware and Network Servicing Level V**	
Unit Title	**Establish and Maintain Client User Liaison**
Unit Code	**EIS HNS5 04 1221**
Unit Descriptor	This unit defines the competency required to establish and maintain client user liaison in an IT environment, post implementation. This occurs after the business-critical functions have been determined.

Elements	Performance Criteria
1. Determine support areas	1.1 Information technology used in the organisational unit is identified and recorded. 1.2 ***Stakeholders*** of the ***system*** are identified. 1.3 Organisational structure, culture and politics are identified in relation to support requirements. 1.4 Level of support required by each organisational unit is determined
2. Develop support procedures	2.1 Organisational units are contacted, as required, to verify support needs. 2.2 Procedures are established for providing required support, including method of contact, frequency of meetings and reports 2.3 Agreed procedure, ***service-level agreement***, is documented.
3. Assign support personnel	3.2 IT skills required to assist each organisational unit are identified with support activities. *3.3* Personnel are assigned according to human resource processes. 3.4 Availability of selected personnel is verified.

	3.5 Support is provided using agreed procedures. 3.6 Feedback is obtained from the ***appropriate person*** on a regular basis.

Variable	**Range**
Stakeholders	May include • sponsor • user • development team • project team
System	May include but is not limited to • databases • applications • servers • operating systems • gateways • application service provider (ASP) and ISP
Service-level agreement	May exist for many different infrastructure services, including • communications carriers • ISPs • ASPs • SLAs for vendor products SLAs should consider business processes and requirements, clearly specify and quantify service levels, identify evaluation or audit of service levels. May include • workload and performance considerations • expectations regarding servicing • penalties • charge back to business units
Appropriate person	May include • supervisor • teacher • authorised business representative or client

Evidence Guide	
Critical Aspects of Competence	Demonstrates skills and knowledge in: • Ability to establish and maintain client liaison in an IT environment. • Evidence of communication and reporting mechanisms consistent with the identified role and as agreed between the parties must be demonstrated.
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • General knowledge of the role that IT plays in the client's business domain. Knowing what equipment supplies business-critical services (e.g. web server for e-business, internet file transaction security for client accounts) • Awareness of who the stakeholders are, what role they play in the organisation and how dependent they are on the IT infrastructure (e.g. salespeople and other mobile workforces may need a remote access communication service while travelling.) • Detailed knowledge of the IT system's current functionality in supplying the essential and desirable services to the organisation. (e.g. what servers are engaged in providing the services such as email, web, proxy, firewall, back-up) • Broad knowledge of quality assurance practices in relation to how the service is supplied (e.g. are response times for help desk issues adequate for maintaining the organisation's desired business activity level?) • Current industry-accepted hardware and software products, capabilities of IT devices, and detailed knowledge of areas related to the organisation's services, (e.g. specialised knowledge of website security, dynamic data exchange or on-line open file back-up system).
Underpinning Skills	Demonstrates skills to: • Plain English literacy and communication skills in relation to analysis, evaluation and presentation of information such as reporting on service history issues are necessary. These could be in response to particular problems or in response to an approach to quality assurance processes aimed at a general improvement. • Teamwork skills involve the contribution to solutions and goals of a non-routine or contingency nature (e.g. when a major system upgrade is needed and a workgroup approach is employed to implement it). • Group facilitation and presentation skills in relation to transferring and collecting information and gaining consensus on concepts, such as when there are alternatives to decide upon, in installing new technology or in altering the service process for the current system.

	• Project planning skills in relation to how to deliver on scope, time, cost and quality, and how to promote communications and manage risk. • Negotiation skills in relation to other team members and applied to a defined range of predictable problems, such as organising equitable workloads for each team member when extra (weekend or night) work is necessary for a major network upgrade. • Report writing skills for business, requiring depth in some areas, analysis and evaluation of information in a defined range of areas (e.g. outlining possible alternatives in technology or equipment changes). • Customer service skills, including a semi-educational role when dealing with end-user problems, so that, by explaining relevant concepts, the learner can empower the end-user to attempt remedial action, the next time a similar problem occurs.
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices. • Service-level agreements • Documented support requirements
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level V	
Unit Title	**Match IT Needs with the Strategic Direction of the Enterprise**
Unit Code	**EIS HNS5 05 1221**
Unit Descriptor	This unit defines the competency required to ensure IT services meet current and future internal operational enterprise requirements

Elements	Performance Criteria
1. Evaluate current business strategy	1.1 Current strategic plan of organization is analyzed to understand the industry environment and current organizational goals. 1.2 Information related to current operational practices and the strategic plan is compared to determine possible IT gaps and improvement opportunities. 1.3 Information regarding the impact of IT developments is reported to ***appropriate person(s)***
2. Evaluate impact of changes	2.1 Information on current IT systems supported by the organization is reviewed. 2.2 Advantages and disadvantages of current and proposed IT systems are compared and documented. 2.3 The objectives and implications of introducing changes are determined. 2.4 Findings are document and forward to appropriate person(s) for feedback.
3. Develop action plans	3.1 Action plans are developed for the proposed changes that can be implemented according to organizational policies and procedures

	3.2 Action plans that take account of appropriate operational, financial, legal, human relations, internal and external operating environments and other relevant considerations are ensured. 3.3 Document action plans, ensuring that standards, targets and implementation methods are detailed 3.4 Documentation is forwarded to appropriate person for feedback/approval.

Variable	**Range**
Appropriate person	May include but not limited to: • supervisor, • authorized business representative or client

Evidence Guide	
Critical Aspects of Competence	Demonstrates skills and knowledge in: • accessed and analyzed relevant information on changes to technology and resources; • analyzed strategic plans to determine future technology needs; • monitored resource utilization and cost efficiency and effectiveness of technology • Developed action plan
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • Broad knowledge of technology and product directions for evaluating and forecasting vendor and technology trends • Analysis and planning approaches to technical problems or management requirements, taking into account the hardware platform used by the organization, and network and security guidelines • Broad knowledge for evaluating current system functionality to forecast for planning • Broad knowledge for evaluating internal and external operating environments • Broad knowledge for evaluating the operating systems supported by the organization to forecast for planning
Underpinning Skills	Demonstrates skills to:

	• Negotiation skills in relation to planning and selecting appropriate equipment and services for self and others, such as when planning for client support service delivery within quality, time and cost parameters • Evaluation and report writing skills involving analysis for evaluating IT changes, documenting recommendations and developing action plans • Evaluation skills to determine possible IT client support gaps • Broad strategic planning skills in relation to current operational practices and future requirements and the implications of introducing IT changes • Planning and analysis skills for reviewing objectives and performance measures • Time management skills in relation to planning the management of client support services • Organizing and presenting information in relation to business report writing requirements
Resources Implication	To demonstrate competency in this unit the learner will require access to: • Detailed information relating to business strategic plan • Budget constraints • A timeframe for the strategic plan • Business objectives • Business risks • Information on a range of IT business solutions
Methods of Assessment	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level V	
Unit Title	**Install, configure and test a router**
Unit Code	**EIS HNS5 06 1221**
Unit Descriptor	This unit describes the performance outcomes, skills and knowledge required to undertake router installation and configuration as part of the upgrade in an existing network or the implementation of a new network.

Element	Performance Criteria
1. Prepare to install a router	1.1. Prepare for given work according to relevant legislation, occupational health and safety (OHS), codes, regulations and standards 1.2. Arrange access to the site according to required procedure 1.3. Ascertain ***network*** topology from technical requirements 1.4. Determine the internet protocol (IP) addressing scheme for the network topology 1.5. Evaluate network management and security ***requirements***, with reference to current and future requirements 1.6. Select a ***router*** with appropriate features according to technical requirements 1.7. Choose ***cables***, wireless application protocol (WAP), wide area network (WAN) connectors and other ***peripherals/tools*** according to network and router specification, and ***WAN protocols***
2. Install and configure a router	2.1. Assemble router and peripherals according to manufacturer's requirements, enterprise guidelines and ***protocols***

	2.2. Connect communications cables and WAN connectors to the router and to the network 2.3. Configure router according to manufacturer's instructions and technical requirements, taking into account interoperability requirements with network components 2.4 use and work on ***Simulation*** software at the absence of real router
3. Test the router and reconfigure the network	3.1. Test the router for connectivity across the network and for ***routing protocol*** functions 3.2. Adapt or modify the predetermined router configuration, depending on outcome of tests 3.3. Review router in line with organisational requirements 3.4. Test router and peripherals according to manufacturer's instructions and technical requirements 3.5. Test ***hardware*** and router to ensure full functionality and interoperability 3.6. Reconfigure additional hardware as required 3.7. Make adjustments to network depending on test results
4. Complete documentation and clean-up worksite	4.1. Tabulate test results and complete all user reports 4.2. Complete report and notify client of status of the network 4.3. Clean up and restore worksite to client's satisfaction 4.4. Secure sign off from ***appropriate person***

Variable	**Range**
Network may include:	• Data • internet • internet protocol private branch exchange (IP PBX) • internet protocol TV (IPTV) • large and small LANs • national WANs • radio frequency identification (RFID) • storage area network (SAN) • voice • voice over internet protocol (VoIP) • Virtual private network (VPN).
Requirements may be in reference to:	• application • business • network • employees in the organisation • System.

Router may include:	• 3Com Office Connect Remote 810 ADSL • 3Com Super Stack 400 • Cisco 800 and ISR Series routers • Cisco uBR7200 universal broadband routers • Cisco wireless access points • D-Link routers • Intel Express series • Juniper routers • Linksys routers • Motorola Vanguard series • Netopia routers.
Cables may include:	• Category 5e, 6 or 7 • crossover • fibre • shielded twisted pair (STP) • straight through • Unshielded twisted pair (UTP). • Coax
peripherals/tools may include:	• Bluetooth devices • fax • Fire wire (IEEE 1394) • input equipment: • keyboard • mouse • pens • touch pad • laptops and desktop computers • mobile phones • modems • multimedia kits • palmtops and personal digital assistants (PDAs) • personal computer • printers • scanners • speakers • tape cartridges • Universal serial bus (USB) • router configuration application

	• Putty • Mobaxterm etc…
Simulation	• May include but not limited: • CISCO packet tracer • ENSP • GNS or other
WAN protocols may include:	• advanced data communications protocol (ADCP) • binary synchronous control (BSC) • high-level data link control (HDLC) • point to point protocol (PPP) • synchronous data link control (SDLC) • transmission of IP datagrams over X.25, Frame Relay or ATM.
Protocols may include:	• AppleTalk protocol - Phase 2 (1989) • dynamic host configuration protocol (DHCP) • novell protocol suite: • internetwork packet exchange (IPX) • NetBIOS emulator • netware core protocol • sequenced packet exchange (SPX) • TCP/IP: • internet control message protocol (ICMP) see router protocols above • Net BT • WAN protocols (encapsulations): • advanced data communications protocol (ADCP) • binary synchronous control (BSC) • high-level data link control (HDLC) • point-to-point protocol (PPP) • Synchronous data link control (SDLC).
Routing protocol may include:	• Cisco discovery protocol (CDP) • dynamic routing • enhanced interior gateway routing protocol (EIGRP) • exterior gateway protocol and border gateway protocol (superseded by BGP) • netWare link state protocol (NLSP) • open shortest-path first interior gateway protocol (OSPF) • routing information protocol (RIP) • Static routing.

Hardware may include:	• DSL modems • modems and other connectivity devices • networks • personal computers • remote sites • servers • Workstations.
Appropriate person may include:	• authorised business representative • client • Supervisor.

Evidence Guide	
Critical Aspects of Competence	Demonstrates a knowledge and skills of: • plan and prepare for the router installation task • select a router to meet the client business specifications • install and test the router that ensures interoperability within the network and applying router principles and technologies • report on the status of the completed installation and seek sign off and customer satisfaction • use routers • Apply solutions to defined routing problems.
Required Knowledge and Attitudes	Demonstrates knowledge of: Australian Computer Society Code of Ethics effect of a router on delimiting broadcast traffic and on conserving bandwidth how dynamic routing algorithms or protocols create and maintain routing tables providing the network with redundant paths for reliability and the way routers manage these paths router: 1) basic router commands 2) configuration: 1. clock rate 2. password protection of router 3. routing protocol 3) dynamic routing 4) firewalls 5) functions
Required Skills	Demonstrates skills to:

	• communication skills to liaise with internal and external personnel on technical, operational and business related matters • literacy skills to interpret technical documentation and write reports in required formats • numeracy skills to take test measurements, interpret results and evaluate performance and interoperability of network • planning and organisational skills to plan, prioritise and monitor own work and coordinate the process in liaison with others • problem solving and contingency management skills to adapt configuration procedures to requirements of network and reconfigure depending on differing operational contingencies, risk situations and environments • research skills to interrogate vendor databases and websites to implement different configuration requirements to meet security levels • technical skills to select and use router test software and hardware to suit different network applications • routing protocols and how they operate tables router-based network architectures • use of routing tables in intelligent packet routing and switching
Resource Implications	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Methods of Assessment	Competence may be assessed through: • Interview / Written Test • Observation / Demonstration with Oral Questioning
Context of Assessment	Competence may be assessed in the work place or in a simulated work place setting.

TOP

Occupational Standard: Hardware and Network Servicing Level V	
Unit Title	**Install and manage complex ICT networks**
Unit Code	**EIS HNS5 07 1221**
Unit Descriptor	This unit describes the performance outcomes, skills and knowledge required to install and manage enterprise-wide information and communications technology (ICT) networks.

Element	Performance Criteria
1. Plan and design a complex network to meet business requirements	1.1 Review network design, business requirements and latest vendor technical specifications for ***network components***
	1.2 Research options available for providing the network functionality required
	1.3 Plan network implementation to provide ***network services*** and ***resources*** to meet business requirements
2. Design and implement a security strategy	2.1 Analyse requirements for internal and external security
	2.2 Design ***security strategy*** to meet requirements
	2.3 Implement security strategy
	2.4 Undertake ongoing monitoring of the viability and reliability of network security, through testing and use of technical ***tools***
	2.5 Continually monitor internal and external network access for security breaches
3. Install and configure a complex network to meet business requirements	3.1 Check and install cabling and associated components according to industry standards
	3.2 Install and configure servers, routers, switches or other devices to provide internet protocol (IP) addressing and routing
	3.3 Install and configure servers, routers, switches or other devices to provide name resolution
	3.4 Install and configure servers, routers, switches or other devices to provide network services
	3.5 Install and configure remote access services
	3.6 Install and configure devices to provide ***data management services***
4. Provide integrated network services across a complex network	4.1 ***Integrate multiple network services*** across network
	4.2 Analyse and resolve interoperability issues
	4.3 Optimise performance

	4.4 Rectify security conflicts arising from integrating services
5. Plan, design and implement voice and video business communications system	5.1 Install software and configure and test voice over internet protocol (VoIP) and videoconferencing services 5.2 Incorporate the use of a communications server to provide real-time multimedia communications 5.3 Select common voice and videoconferencing codecs according to standards and practices
6. Manage and support a complex network	6.1 Identify and evaluate appropriate network management tools to assist in the administration of the complex network 6.2 Select and install network management tools according to industry and organisational standards 6.3 Set and monitor alerts and logs 6.4 Capture and analyse network performance data 6.5 Implement automated server updates 6.6 Implement desktop management policies 6.7 Implement automated virus checking 6.8 Use remote management tools
7. Test network functionality and obtain sign-off	7.1 Test network functionality and record results 7.2 Record results of network functionality test 7.3 Complete network documentation according to organisational standards

Variable	**Range**
Network components may include:	• cables • digital subscriber line (DSL) modems • local area network (LAN) • modems • routers • servers • switches • WAN • Wireless access point.

Network services may include:	• database service • DHCP • DNS • FTP • firewall • hypertext transfer protocol (HTTP, HTTPS) • internet message access protocol (IMAP) • network file system (NFS) • NTP • post office protocol (POP) • print services • proxy • SMB • simple mail transfer protocol (SMTP) • simple network management protocol (SNMP) • Transmission control protocol or internet protocol (TCP/IP).
Network resources may include:	• backup and data security • business applications • collaboration tools • conferencing • data storage • databases • email • internet services • printers, faxes and scanners • streaming video • VoIP.
Security strategy may include:	• automated updates: • Red Hat Network (RHN) • Windows Server Update Services (WSUS) • encryption • Firewall - demilitarised zone (DMZ) • proxy • public key infrastructure (PKI) and secure socket layer (SSL) certificates • secure remote access • server hardening • smart cards • tokens • user authentication • virus checking • VPN.

Tools may include:	• cable testing • carrier connection tests • data and voice integration measurements • equipment testing • frequency analysers • network performance software • packet tracers • Policing and shaping tools.
Data management services may include:	• backup and recovery • disk quotas • distributed file systems • indexing • online and offline storage • Storage area networks (SANs).
Integrate multiple network services may include:	• Kerberos • lightweight directory access protocol (LDAP) • Samba • seamless access to Linux and Windows hosted data and services • single login to gain access to multiple services (federated authentication) • VoIP over VPN.

Evidence Guide	
Critical Aspects of Competence	Evidence of the ability to: • design and implement a complex network that involves integrating multiple network services to meet business requirements • design and implement an appropriate security strategy for a complex network • monitor and test the performance of aspects of the solution • Provide ongoing management and support of the network.
Required Knowledge and Attitudes	Demonstrates knowledge of:

	• firewall configuration
	• IP addressing and network configuration
	• network:
	  • infrastructure
	  • load-balancing for applications
	  • security
	  • server operating systems
	  • service configuration, including:
	  • DNS
	  • dynamic host configuration protocol (DHCP)
	  • file transfer protocol (FTP)
	  • mail network time protocol (NTP)
	  • proxy
	  • server messages block (SMB)
	  • web service management
	• troubleshooting tools and techniques, including network diagnostic utilities
	• user authentication and directory services
	• VoIP
	• VPN

Required Skills	• analytical skills to use complex technical data to develop network designs
	• communication skills to consult with customers
	• literacy skills to:
	  • interpret technical documentation
	  • write reports
	• numeracy skills to:
	  • take test measurements
	  • interpret results
	  • evaluate performance and interoperability of network services
	• problem-solving skills to solve a range of predictable network problems
	• research skills to identify, analyse and evaluate broad features of a particular business domain and best practice in networking technologies, including hardware and software to be installed
	• technical skills to:
	  • implement dynamic name system (DNS), IP addressing and secure virtual private network (VPN) tunnels
	  • install and configure application software to provide specific services
	  • install, configure and secure server operating systems
	  • install, configure and secure switches and routers
	  • integrate multiple network services without conflict
	  • set up and use network monitoring and management tools
	  • Test network functionality.

Resource Implications	• network design and business requirements documents • a complex network or hardware and software required to build a network involving multiple servers, multiple physical locations (or simulation of) and a combination of network services • Appropriate learning and assessment support when required. Where applicable, physical resources should include equipment modified for people with special needs. And practices.
Methods of Assessment	Competence may be assessed through: • Interview / Written Test • Observation / Demonstration with Oral Questioning

Context of Assessment	Competence may be assessed in the work place or in a simulated work place setting.

TOP

Occupational Standard: Hardware and Network Servicing Level V	
Unit Title	**Plan and Monitor the System Pilot**
Unit Code	**EIS HNS5 08 1221**
Unit Descriptor	This unit defines the competency required to test and evaluate the developed system among a subset of clients to gauge reaction and gather feedback.

Elements	Performance Criteria
1. Prepare for pilot system	1.1 Objectives, success criteria and ***acceptance criteria*** are established and confirmed for pilot implementation 1.2 Technical and ***organizational resources*** required for ***pilot*** implementation are identified and secured. 1.3 Executive support for pilot is established and confirmed. 1.4 Project plan for pilot is completed and project documentation is referred to appropriate person for approval
2. Install pilot system	2.1 Pilot is installed and configured according to ***project plan*** 2.2 Technical readiness of pilot is verified and recorded. 2.3 Necessary actions is taken to ascertain accuracy of data. 2.4 A status report is prepared and submitted to appropriate person for sign-off.
3. Monitor implementation of pilot system	3.1 Pilot and support documentation is reviewed, to ensure complete understanding. 3.2 Pilot and system procedures is Identified. 3.3 System functionality and integrity tests is supervised 3.4 Document findings 3.5 Appropriate technical support is provided as required.
4. Evaluate pilot system	4.1 Pilot objectives and success criteria is reviewed against pilot operation 4.2 Client and executive feedback on pilot is reviewed against ***acceptance criteria*** 4.3 Areas of success and improvement are Identified and prioritized 4.4 Assess the impact of changes on the pilot 4.5 Document review process and submit to appropriate person

Variable	Range
Acceptance criteria	May include but not limited to: • timeframe • cost implications • technical • logistical considerations
System	May include but is not limited to • Databases • Applications • Servers • Operating systems • gateways, • application service provider and ISP
Pilot	Details of pilot will vary according to • organizational requirements • Nature of system. • All system pilots will take an iterative approach and involve users in the process
Client	May include but is not limited to • internal departments, • external organizations, • individual people and • internal employees
Organizational resources	• Will vary, subject to nature of pilot. • Staffing resources would be expected from user community, technical operations, technical support, technical development, supplier, project manager and executive sponsor. • Financial resources will need to be secured to fund the pilot. • Systems developers and IT technicians • Representative experts from relevant business areas (e.g. functional • managers or operational staff) • Representative users • Personnel with an understanding of corporate governance (e.g. legal, audit and data security specialists)
Acceptance criteria	May include • timeframe, • cost implications, • technical, • accessibility and • logistical considerations

Appropriate person	May include a • supervisor, • teacher, • authorized business representative • Client.
Project plan	May include a number of variables, including parties and their responsibilities, • project scope, • project objectives, • Schedule, • Project budget, etc.

Evidence Guide	
Critical Aspects of Competence	Demonstrates skills and knowledge in: • Prepared for pilot system • Installed pilot system • Monitored implementation of pilot system • Evaluated pilot system
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • Current industry-accepted system piloting methodologies, with knowledge of general features and capabilities • Current industry system development and design methodologies (e.g. when preparing for pilot) • Current industry-accepted hardware and software products, with broad knowledge of general features and capabilities and detailed knowledge in some areas (e.g. when installing pilot system) • Project objectives and client requirements (e.g. when monitoring implementation of pilot) • Overall project objectives and client requirements (e.g. when preparing for pilot) • Client business domain • Three or more current industry information gathering methodologies (e.g. when preparing for pilot) • Role of stakeholders and the degree of stakeholder involvement • System's current functionality (e.g. when installing pilot system) • Quality assurance practices
Underpinning Skills	Demonstrates skills to: • Problem solving skills for a defined range of unpredictable problems involving participation in the development of strategic initiatives (e.g. when technical and organizational

	resources required for pilot implementation are identified and secured in a timely manner)) • Plain English literacy and communication skills in relation to analysis, evaluation and presentation of information (e.g. when training and user participants' exposure to joint application development (JAD) process is facilitated) • Project planning skills in relation to scope, time, cost, quality, communications and risk management (e.g. when project plan for pilot is completed and authorization obtained from higher authorities) • Group facilitation and presentation skills in relation to transferring and collecting information and gaining consensus on concepts • Research skills for identifying, analyzing and evaluating broad features of a particular business domain and best practice in system piloting (e.g. when organizational procedures used for the pilot are documented) • Teamwork skills involving the contribution to solutions and goals of a non-routine or contingency nature (e.g. when client user and executive feedback on pilot are reviewed against acceptance criteria)
Resources Implication	To demonstrate competency in this unit the person will require access to: • Acceptance criteria • Pilot plan • Effective assessment of this competency requires access to: • A pilot system • Project plan • Technical materials and • People to be involved in the pilot
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

NQTF Level IV

TOP

Occupational Standard: Hardware and Network Servicing Level IV	
Unit Title	**Provide network systems administration**
Unit Code	**EIS HNS4 01 1221**
Unit Descriptor	This unit describes the performance outcomes, skills and knowledge required to technically manage elements of a network, including contributing to disaster recovery plan.

Element	Performance Criteria
1. Provide client access and security	1.1 Provide logons, passwords and applications file access to ***users*** and prepare ***documentation*** in line with ***organisational requirements*** 1.2 Examine records of user accounts to determine access privileges and usage 1.3 Take necessary action to ensure maintenance of ***system*** integrity and security
2. Provide input into and disseminate disaster recovery plan	2.1 Provide input into the organisation's ***disaster recovery plan*** 2.2 Disseminate disaster recovery plan to users as required
3. Monitor network performance	3.1 Perform diagnostic tests associated with administering the network or system 3.2 Analyse and respond to diagnostic information 3.3 Monitor ***software*** usage, including inappropriate or illegal use 3.4 Delete illegal software from the system 3.5 Monitor ***hardware*** response time and other performance indicators 3.6 Determine and action methods for improving network and systems efficiency according to ***organisational guidelines***
4. Migrate to New Technology	4.1 Situations are identified where existing knowledge can be used as the basis for developing new skills. 4.2 New or upgraded technology skills are acquired and used to enhance learning and ***equipment*** are identified, classified and used where appropriate, for the benefit of the organization. 4.3 Features of new or upgraded equipment *are* and ***software*** applied within the organization 4.4 Features and functions of new or upgraded equipment is used for solving organizational problems 4.5 ***Sources of information*** is accessed and used relating to new or upgraded equipment

	4.6 ***Feedback*** is sought from users where appropriate.

Variable	Range
Users may include:	• Contractors • departments within an organisation • persons within a department • support staff • Third parties.
Documentation may follow:	• audit trails • client training • equipment inventory maintenance • International Organization for Standardization (ISO), International Electro technical Commission (IEC) and Australian Standards (AS) standards • naming standards • project-management templates and report writing • satisfaction reports • Version control.
Organisational requirements may be in reference to:	• diagnostic policy • preventative maintenance • problem solution processes • roles and technical responsibilities in the IT department • vendor and product service level support agreements • work environment.
System may include:	• application • business • computers • financial system • information system • management system • network • software.
Disaster recovery plan may include:	• backup plans • disaster recovery activities • impact assessment • key roles and responsibilities • maximum tolerable outage • recovery time • risk analysis • zero data loss.

Software may include:	• application:
	  • database
	  • internet browser
	  • spreadsheet
	  • word-processing
	• commercial
	• customised
	• in-house
	• programming:
	  • assembler
	  • compiler
	  • development tools
	• system:
	  • computer security
	  • device drivers
	  • Operating system.

Hardware may include:	• modems or other connectivity devices • networks • personal computers • remote sites • servers • Workstations.
Organisational guidelines may include:	• communication methods • content of emails • dispute resolution • document procedures and templates • downloading information and accessing particular websites • financial control mechanisms • opening mail with attachments • personal use of emails and internet access • Virus risk.

Evidence Guide	
Critical Aspects of Competence	Demonstrates a knowledge and skills of: • sustain the operation of the network through maintenance of network integrity and perform diagnostic tests • contribute to the formulation of a disaster recovery plan and provide the client with an optimized network that complies with organisational guidelines • improve network and systems efficiency according to organisational guidelines • provide appropriate access to the network for users

	• Maintain, limit or enhance user access according to authorised requests.
Required Knowledge and Attitudes	Demonstrates knowledge of: • approaches to backup and restoring computer data • disaster recovery policy • features and functions of file access • in-house and vendor support • OHS legislation relating to the use of equipment • operating systems: ▪ functions and basic features ▪ supported by the organisation • organisational access and security procedures • organisational and technical systems • organisational procedures for protection against and elimination of computer viruses • policy and procedures • advanced knowledge of software features supported by the organisation for deleting, restoring and archiving files • procedures for creating logons • security and network guidelines and procedures • Software copyright responsibilities.
Required Skills	Demonstrates • communication skills to: ▪ investigate and assess client needs ▪ provide one-to-one instruction customer-service skills to communicate with clients in a range of contexts at various levels • literacy skills to: ▪ develop reports ▪ interpret technical manuals • planning and organisational skills to provide input into the disaster recovery plan • technical skills to perform: ▪ diagnostic tests to monitor network performance ▪ System administration tasks.
Resource Implications	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Methods of Assessment	Competence may be assessed through: • Interview / Written Test • Observation / Demonstration with Oral Questioning
Context of Assessment	Competence may be assessed in the work place or in a simulated work place setting.

TOP

Occupational Standard: Hardware and Network Servicing Level V	
Unit Title	**Develop System Infrastructure Design Plan**
Unit Code	**EIS HNS4 02 1221**
Unit Descriptor	This unit defines the competency required to specify the hardware, network, software and infrastructure required to support the system.

Elements	Performance Criteria
1. Specify architecture requirements	1.1 Critical principles, functions and framework for the ***system*** to operate across business units, are identified. taking into account the project deliverables, acceptance criteria and current IT blueprint 1.2 Functions are organised into layers or wrappings and components to meet ***business requirements***. 1.3 Processing environment, the ***hardware***, ***network*** and software required to support the operational environments are identified. 1.4 The system topology model, templates and standards are refined to guide development 1.5 The ***project*** guidelines, standards, models, acceptance criteria and general framework are utilised to develop the architecture
2. Specify hardware and software	2.1 Various products and vendors are evaluated against the requirements of the architecture to determine the best IT solution. 2.2 Current and future capacity requirements are estimated and evaluated against client future requirements. 2.3 Requirements are identified for upgrade or change through analysis of ***software*** versions and interoperability status of existing system and applications.
3. Conduct walk-through and compare/ contrast expected performance	3.1 Requirements model are compared against technical specifications and ***acceptance criteria***. 3.2 Requirements model are compared against vendor proposed offering 3.3 The requirements model benchmarked against current industry standards and IT blueprint for performance, interoperability and expected future organisational requirements.

4. Document and report on findings	4.1 System infrastructure design plan are prepared including hardware, network, software and general infrastructure aspects 4.2 Recommendations are documented and referred to the appropriate person for improvement.

Variable	Range
System	May include • Databases • Applications • Servers • operating systems • gateways • ASP • ISP
Acceptance criteria	May include • Timeframe • cost implications • technical and logistical Considerations
Business requirements	May be in reference to • the business • system • application • network or people in the organisation
Hardware	May include but is not limited to • workstations • personal computers, Laptop and PDA • modems and other connectivity devices • networks • ADSL modems • remote sites • servers
Project	May include a • total organisational change • a systems-only change • a business improvement process • e-business solution involving the total organisation or part of the organisation
Standards	May include • ISO/IEC/AS and relevant standards • organisational standards • project standards
Software	May include but is not limited to • commercial Software

	• in-house developed Software • Packaged or customised Software etc…
Network	May include but is not limited to • large and small LANs, MAN, WANs • the internet • PSTN for dial-up modems • CDMA 1X • EV-DO • Handy Wi-fi Router(ZTE, Huawei) • private lines • VPNs • data and voice • Current Internet Technologies
Architecture	May include but is not limited to: • Operating system: any operating system that has multi-user ability, Linux, Mac OS, Windows 7 or above • Database software: Oracle, Sybase, Microsoft SQL server, Ingres, DB2,Informix, MySQL, SQL server • Configuration: small memory model, large memory model, requests per second
requirements	Requirements may be in reference to • the business • system • application • network • people in the organisation
Solution	May include but is not limited to • new hardware, • hardware upgrades, • new software, software upgrades, • user training • implementing a new system
Client	May include but is not limited to • internal departments, • external organisations, • individual people • employees
Applications	May include but are not limited to • commercial software applications; • organisation-specific software; • word processing, • spreadsheet, • database, • graphic • communication packages May include presentation applications contained in:

	• Microsoft Office • Lotus Suite • Office 365
Specifications	May include but are not limited to • technical requirements • user problem statement • current system functionality
Documentation	May follow • ISO/IEC/AS and relevant standards • audit trails • naming standards • version control • project management • report writing conventions • maintaining equipment inventory • client training • satisfaction reports
Organisational requirements	May be in reference to • the business • system • application • network • people in the organisation

Evidence Guide	
Critical Aspects of Competence	Demonstrates skills and knowledge in: • Specified hardware and software • Conducted walk-through and compared/contrasted expected performance criteria against vendor proposed offerings • Documented and reported on findings
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • Current industry-accepted hardware and software products • Broad general knowledge of the client business domain, particularly the business function and organisation (e.g. when specifying architecture requirements) • Basic knowledge of cabling and telecommunications technologies (e.g. when specifying architecture requirements) • Broad knowledge of vendor product directions and technology directions (e.g. when specifying hardware and software) • Networking technologies, including broad knowledge of general features and capabilities incorporating substantial depth in some areas (e.g. when specifying architecture requirements)

	• Broad knowledge of systems architectural design principles and methodologies (e.g. when specifying architecture requirements • Broad knowledge of modelling techniques and methodologies (e.g. when specifying architecture requirements, and for comparing and contrasting after walk-through of expected performance criteria against vendor proposed offerings)
Underpinning Skills	Demonstrates skills to: • Problem solving skills for a broad range of unpredictable problems involving analysis, diagnosis and evaluation (e.g. when specifying the critical principles, functions and framework for the system to operate across the enterprise or business units, taking into consideration the project deliverables, acceptance criteria and current IT blueprint) • Plain English literacy and communication skills in relation to analysis, evaluation and presentation of information (e.g. when the initial statement of hardware needs is written) • Group facilitation and presentation skills in relation to transferring and collecting information (e.g. when estimating current and future capacity requirements and evaluating against client's future requirements, and for documenting recommendations for improvement and referring them to appropriate technical specialists) • Questioning and active listening skills (e.g. when specifying the critical principles, functions and framework for the system to operate across the enterprise or business units, taking into consideration the project deliverables, acceptance criteria and current IT blueprint) • Technological capability assessment skills involving analysis, diagnosis and evaluation (e.g. when evaluating various products against architecture requirements to determine the best IT solution, and for estimating current and future capacity requirements and evaluating against client's future requirements) • Research skills for specifying, analysing and evaluating broad features of a particular business domain and best practice in system development (e.g. when evaluating various products against architecture requirements to determine the best IT solution, and for benchmarking requirements model against current industry standards and IT blueprint for performance, interoperability and expected future organisational needs) • Project planning skills in relation to set benchmarks and identified scope (e.g. when specifying the critical principles, functions and framework for the system to operate across the enterprise or business units, taking into consideration the project deliverables, acceptance criteria and current IT blueprint)

	• Report writing skills for business requiring depth in some areas, analysis and evaluation of information in a defined range of areas (e.g. when documenting recommendations for improvement and referring them to appropriate technical specialists)
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices. • Client requirements • The project deliverables • The acceptance criteria • Current IT blueprint • Information on a range of IT business solutions and vendor offerings • Future organisational business process requirements • Technical specifications
Methods of Assessment	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level IV	
Unit Title	**Build Internet Infrastructure**
Unit Code	**EIS HNS4 03 1221**
Unit Descriptor	This unit defines the competence required to design and implement an infrastructure for internet services

1. Plan and design internet infrastructure	1.1 Internet infrastructure is selected in line with business and end-user requirements, within budget limitations. 1.2 The internet service is evaluated for satisfactory performance and confirmed that the service meets business and end-user requirements. 1.3 ***Hardware*, *software***, ***network*** and security requirements are ensured in accordance with agreed business and end-user specifications. 1.4 Internet protocol address allocation is determined based on the number of addresses needed.
2. Install and configure internet infrastructure and services	2.1 Cables is installed and tested where appropriate according to the standard. 2.2 Mail servers is built and tested when needed. 2.3 Workstation software is installed and configured to access ***services*** 2.4 Necessary hardware and software is installed to connect the internet to intranets or network if required. 2.5 Domain names and internet protocol addresses is configured to make internet access possible. 2.6 Software is set up to provide services as required. 2.7 Software is installed and configured that provides internet links with existing ***databases***, documents and files.
3. Test security and internet access	3.1 Security access levels is tested and verified based on security policy. 3.2 Capability and reliability of security systems is monitored and evaluated based on security policy. 3.3 Changes are made to system to ensure protection against known and potential ***threats***. 3.4 Availability of the internet access to all clients is confirmed

4. Ensure user accounts are verified for security	4.1 User settings are verified to ensure that they conform to security policies. 4.2 Legal notices are displayed at appropriate locations for system users. 4.3 Passwords are checked in accordance with business policies and verified with software utility tools.
5. Manage and support internet	5.1 Management is assisted in developing procedures and policies for maintaining the internet infrastructure. 5.2 Management or Monitoring tools are obtained, installed and used to assist in internet administration. 5.3 Traffic, appropriateness of broadcasts, content access and hits are monitored over the internet. 5.4 Internet performance is optimized in accordance with business need.
6. Plan and Organize Work	6.1 Objectives are consistent with and linked to work activities in accordance with organizational aims. 6.2 Objectives are stated as measurable targets with clear time frames 6.3 Tasks/work activities to be completed are identified and prioritized as directed 6.4 Schedule of work activities is coordinated with personnel concerned 6.5 Work plans are implemented in accordance with set time frames, resources and standards.

Variable	**Range**
Hardware	May include but is not limited to: • Workstations, personal computers, Mobiles, Tablets, modems and other connectivity devices, networks, DSL modems, remote sites, servers.
Software	May include but is not limited to commercial software applications; organization-specific software, packaged software, in-house or customized software
Network	May include but not limited to: • Large and small LANs, national WANs, the internet, VPNs, the use of the PSTN for dial-up modems only, private lines, data and voice.
Services	May include newsgroups, email, file transfer protocol facilities, multimedia, conferencing and general access to internal website HTML files.

Databases	May include Oracle, Sybase, Microsoft SQL Server, Ingress, DB2, Informix, mSQL, MySQL, SQL server.
Threats	May include eavesdropping, manipulation, impersonation, and penetration, denial of service and by-pass, hackers, viruses.
Tools and equipment	May include but not limited to: • Server hardware and software • Security policy guidelines • Networking hardware (e.g. switches, cables, router, etc…) • Internet connection • Modem or other connectivity device • Personal computer

Evidence Guide	
Critical aspects of Competence	Demonstrates skills and knowledge in: • internet technologies and that internet technology (both hardware and software) is installed and configured correctly
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • General knowledge of the organization's business needs and functions. • General understanding of LAN-based communications technologies. • Knowledge of internet technologies. • General knowledge of OH&S requirements in relation to working in a safe manner; environmental aspects of work that is undertaken and basic and ergonomic considerations relating in particular to the workstation environment. • Security knowledge, with understanding of general features and capabilities, with limited depth in some areas (e.g., when monitoring security and internet access • General knowledge of vendor product and vendor directions (e.g., when installing and configuring internet infrastructure to meet business requirements) • knowledge of open-source options and software (e.g., Linux-based systems) as well as proprietary software (e.g., Microsoft based systems)
Underpinning Skills	Demonstrates skills to: • establish internet connectivity based on the business requirements of the organization • build internet infrastructure
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.

Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level IV	
Unit Title	**Build a small wireless local area network**
Unit Code	**EIS HNS4 04 1221**
Unit Descriptor	This unit describes the performance outcomes, skills and knowledge required to build and arrange connectivity to a basic wireless local area network (WLAN).

Element	Performance Criteria
1. Confirm client and equipment requirements	1.1 Identify, clarify and organise ***client*** requirements according to network needs and ***organisational requirements***
	1.2 Ensure an appropriate person has given the authority for wireless network access
	1.3 Evaluate requirements along with business needs and translate into technical requirements
	1.4 Identify ***components*** to be installed in order to meet the technical requirements
	1.5 Select position for access point, based on ***user*** requirements and environmental conditions
	1.1 1.6 Arrange for preliminary work to be carried out to meet cabling and power requirements
2. Select, install and configure wireless access point	2.1 Select access point device based on current and future client needs
	2.2 Install and configure access point to provide wireless access to ***network***
	2.3 Configure services
	2.4 Test access point and verify wireless connection and security arrangements
	2.5 Select, install and configure appropriate wireless card where necessary for legacy equipment
3. Configure network	3.1 Configure security and other key parameters consistent with ***commercial and business requirements***
	3.2 Test ***security*** and firewall arrangements with appropriate test equipment
	3.3 Test the network with user equipment for general compatibility and access
4. Train users	4.1 Determine devices to be connected to the network
	4.2 Demonstrate how pairing and log-on arrangements are established to user

	4.3 Inform users of wireless network etiquette and traffic capacity issues 4.4 Develop user ***documentation***
5. Monitor and administer wireless network	5.1 Monitor wireless network performance using diagnostic ***tools*** 5.2 Debug networking issues to maintain trouble-free wireless connection 5.3 Document current settings and store securely

Variable	**Range**
Client may include:	• External organizations • Individuals • Internal departments • Internal employees.
Organizational requirements may include:	• Preventative maintenance and diagnostic policy • Problem-solving processes • Roles and technical responsibilities in network management • Vendor and product service level support agreements • Work environment.
Components may include:	wireless access and software hardware: • asymmetric digital subscriber line (ADSL) modems • antennas and other connectivity devices • mobile equipment • modems • wireless access points • networks • personal computers • power controllers • remote sites • servers • UPS • workstations cabling: • category 5e • category 6 • category 7 • Coaxial and fibre.
User may include:	• department within the organization • person within a department • third party • Community members.

Network may include:	• domestic • Small enterprise WLANs.
Commercial and business requirements may include:	• Availability • backup and recovery of data • confidentiality • firewalls • hacking prevention • integrity • password logons • Remote access to internal network.
Security may include:	• AAA • Diameter • EAP or LEAP • IPSec • PKM • smart cards • SSL • tokens • WEP • WPA or WPA2.
Documentation may follow:	• audit trails • client training • International Organization for Standardization (ISO), International Electro technical Commission (IEC) and Australian Standards (AS) standards • maintaining equipment inventory • naming standards • project management templates and report writing • satisfaction reports • Version control.
Tools may include:	• data and voice integration measurements • Network performance software.

Evidence Guide	
Critical Aspects of Competence	Demonstrates a knowledge and skills of: • develop, implement and maintain wireless networks • install, configure and test wireless access points • test security and network to business specifications • develop user training material • Monitor and resolve wireless network issues.
Required Knowledge and Attitudes	Demonstrates knowledge of:

	features of security threats overview knowledge of: • audit and intrusion detection systems • auditing and penetration testing techniques • authentication methods • network protocols and operating systems • security protocols, standards and data encryption detailed knowledge of: • bandwidth and quality of service • factors affecting signal quality • layer 2 and layer 3 design issues • SOHO • transmission control protocol or internet protocol (TCP/IP) protocols and applications • wireless security strategies • wireless topologies • WLAN solutions.
Required Skills	Demonstrates skills to: • communication skills to liaise with client to determine functional requirements of network • literacy skills to document client requirements • problem-solving skills to troubleshoot and debug: ▪ connectivity issues ▪ security issues • research skills to determine most suitable solution for client • technical skills to: ▪ design, develop and implement various wireless network solutions ▪ implement wireless networking strategies and configure wireless network software and hardware ▪ Implement WLANs.
Resource Implications	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Methods of Assessment	Competence may be assessed through: • Interview / Written Test • Observation / Demonstration with Oral Questioning
Context of Assessment	Competence may be assessed in the work place or in a simulated work place setting.

TOP

Occupational Standard: Hardware and Network Servicing Level IV	
Unit Title	**Manage network security**
Unit Code	**EIS HNS4 05 1221**
Unit Descriptor	This unit describes the performance outcomes, skills and knowledge required to implement and manage security functions throughout a network.

Element	Performance Criteria
1. Define a process for designing security	1.1 Define planning phase for ***network*** security design 1.2 Define building phase for network security design 1.3 Define managing phase for network security design
2. Identify threats to network security	2.1 Determine why ***attacks*** occur 2.2 Determine who the attack may come from 2.3 Analyse common types of network ***vulnerabilities*** 2.4 Determine how attacks occur 2.5 Design a threat model to categorize treats
3. Analyse security risks	3.1 Determine elements of risk management 3.2 Determine ***assets*** that require protection 3.3 Categorise assets and calculate their value to the organisation 3.4 Create a risk management plan
4. Create a security design	4.1 Determine attacker scenarios and threats 4.2 Design ***security*** measures for ***network components*** 4.3 Obtain feedback and adjust if required 4.4 Develop security policies
5. Design and implement responses to security incidents	5.1 Design auditing and incident response procedure 5.2 Document security incidents 5.3 Implement configurations aligned with incident response procedure design 5.4 Test and sign off

Variable	Range

Network may include:	• Data • Internet • local area networks (LANs) • large and small LANs • virtual private networks (VPNs) • wide area networks (WANs) and • Wireless LANs (WLANs).
Attacks and vulnerabilities may include:	• Authorizations • brute force and dictionary attacks • denial of service and by-pass • eavesdropping • hackers • internal threats • intruder detection • manipulation • penetration • social engineering, including impersonation • spoofing • Viruses using logging.
Assets may include:	• Data • hardware • personal information • Product and branding information.
Security may include:	• AAA • Authentication process, Kerberos and challenge handshake authentication protocol (CHAP) • Diameter and remote authentication dial-in user service (RADIUS) • folder and file security • IPSec • lightweight extensible authentication protocol (LEAP) • personal knowledge management (PKM) • smart cards • secure socket layer (SSL) • tokens • VPN • wired equivalent privacy (WEP) • Wi-Fi protected access (WPA) or WPA2.

Network components may include:	• Servers
	• workstations
	• accounts
	• authentication
	• data
	• data transmission
	• network perimeters:
	  ▪ part of router configuration or proxy server
	  ▪ products:
	  • Cisco Centri, PIX
	  • ClearOS
	  • IPcop
	  • Linux iptables
	  • MS ISA server
	  • SmoothWall
	  • Untangle

Evidence Guide	
Critical Aspects of Competence	Demonstrates a knowledge and skills of: • identify threats to security • develop risk management plan • design network security policies • analyse and plan solutions to compromised networks and design incident response • evaluate security information and use it to plan suitable control methods and countermeasures • Add network controls, according to system security policies, procedures and risk management plan.
Required Knowledge and Attitudes	Demonstrates knowledge of:

	• detailed knowledge of: ✓ auditing and penetration testing techniques ✓ logging analysis techniques ✓ organisational network infrastructure ✓ related weaknesses of installed network infrastructure ✓ security technologies • broad knowledge of: ✓ capabilities of software and hardware solutions ✓ emerging security issues ✓ general features of emerging security policies, with depth in security procedures ✓ network management and security process controls • Network security implementation risk management plans and procedures.
Required Skills	Demonstrates skills to: • analytical skills to: ✓ analyse network information ✓ plan approaches to technical problems or management requirements • communication skills to: ✓ convey and clarify complex information ✓ liaise with clients • literacy skills to interpret and prepare technical documentation, including recording security incidents and developing security policies • planning skills to plan control methods for managing system security • problem-solving skills to: ✓ apply solutions in complex networks, including systems processes ✓ deploy rapid deployment of solutions to problems involving failure and security incidents • Technical skills to apply best practice to systems security methodologies and technologies.
Resource Implications	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Methods of Assessment	Competence may be assessed through: • Interview / Written Test • Observation / Demonstration with Oral Questioning
Context of Assessment	Competence may be assessed in the work place or in a simulated work place setting.

TOP

Occupational Standard: Hardware and Network Servicing Level IV	
Unit Title	**Determine Maintenance Strategy**
Unit Code	**EIS HNS4 06 1221**
Unit Descriptor	This unit defines the competence required to determine and operationalize maintenance strategies and supporting processes to achieve continuity of IT operations and business functions.

Elements	Performance Criteria
1. Identify and analyze maintenance needs	1.1 Risks to business continuity are identified due to system malfunction including quantification of possible loss 1.2 ***Systems architecture*** and configuration documentation are reviewed for currency. 1.3 ***Equipment*** and/or ***software*** audit are conducted if appropriate information is not available 1.4 Warranty status of ***component***s and/or software according to vendor, project or organizational requirements are determined and documented 1.5 Critical components and/or software and document recommendations are identified regarding possible service arrangements 1.6 Identified risks and problems are documented. 1.7 Recommended maintenance solutions are developed to meet business needs and applied to deal with the client based on the document
2. Develop service level agreements	2.1 The views and requirements of the ***client*** are determined in order to identify maintenance requirements 2.2 ***Service-level agreement*** is prepared to match client user and business requirements
3. Formulate maintenance strategy	3.1 Maintenance options are examined against cost constraints, risks to business continuity and service-level agreements 3.2 A specific maintenance strategy is identified based on cost, business and service-level agreements requirements 3.3 A preventative maintenance schedule is created based on cost, business and service-level agreements requirements

	3.4 A maintenance strategy is negotiated with client and changes to service-level agreements are made where necessary 3.5 The recommended procedure is documented for approval from appropriate person according to organizational requirements
4. Define client and supplier processes and standards	4.1 Reporting procedures for service requests are negotiated and created with client and suppliers 4.2 Response time standards is determined with client and suppliers 4.3 Escalation procedures is created with client and suppliers 4.4 Help desk or other support function is been set-up in accordance with agreed standards and procedures and in line with industry best

Variable	**Range**
Systems architecture	May include but not limited to: • Operating system: Novell NetWare 5 or above or operating system that has multi-user ability, Linux, Mac OS, Windows 7 or above • Database software: Oracle, Sybase, Microsoft SQL server, Ingres, DB2, Informix, MSQL, MySQL, SQL server • Configuration: small memory model, large memory model, requests per second
Equipment	May include but not limited to: • to workstations, personal computers, modems or other connectivity devices, printers, DSL modems, hard drives, monitors, switches, hubs, personal digital assistant (PDA) and other peripheral devices
Software	May include but not limited to: • in-house, packaged or customized software
Components	May include but not limited to: • CMOS battery, central processing unit (CPU), CD and DVD drives, interface cards, drives, fax/modem cards, RAM upgrades, CPU upgrades
Service-level agreement	May include but not limited to: • May exist for many different infrastructure services, including communications carriers, ISPs, ASPs and SLAs for vendor products. SLAs should consider business processes and requirements, clearly specify and quantify service levels, identify evaluation or audit of service levels. May include workload and performance considerations, expectations

	regarding servicing, penalties, and charge back to business units.
Evidence Guide	
Critical aspects of Competence	Demonstrates skills and knowledge in: • Identifying and analyzing maintenance needs • Developing service level agreements • Formulating maintenance strategy • Defining client & supplier processes & standards
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • Broad knowledge of help desk and maintenance practices, such as general composition and operation of • Information database for tracking hardware, software and operational issues, such as troubleshooting, repair and warranty. Also, knowledge of determining level of support to a client (e.g. support levels one to four) • Current industry-accepted hardware and software products, with broad knowledge of general features and • Capabilities and detailed knowledge in areas pertaining to particular client business activity. (e.g. help desk software, including a database for storing hardware and software details, product warranty and service difficulty records, such as repair, replacement and reconfiguration) • General knowledge of the relationships between the stakeholders and the service provider. This includes • knowing the rights of the stakeholder and the obligations of the learner inferred by the contract of service • Broad knowledge of the client business domain and of the features of the IT system that support the client's business activity • Detailed knowledge of how the system has been set up to process data and what data elements are stored • Broad knowledge of quality assurance practices with reference to maintenance, warranty and repair of network equipment and software
Underpinning Skills	Demonstrates skills to: • Develop service level agreements • Formulate maintenance strategy • Define client and supplier processes and standards
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration

Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level IV	
Unit Title	**Conduct / Facilitate User Training**
Unit Code	**EIS HNS4 07 1221**
Unit Descriptor	This unit defines the competence required to apply techniques that facilitate the working, planning, implementation and monitoring of information technology through training.

Elements	Performance Criteria
1. Plan ICT training system	1.1 Training procedures and aim are researched and developed according to the organizational needs. 1.2 IT training plan are developed 1.3 Staffs/employees, who will take training are identified 1.4 Staff and management are trained in change management procedures and polices 1.5 Current IT training user or business patterns are evaluated 1.6 Key personnel responsible are identified for training and implementing training plan
2. Identify IT system training needs	2.1 Current IT training ***benchmarks*** are determined 2.2 Identified ***needs*** are compared against performance benchmarks to identify possible training 2.3 Proposed training are assessed to determine impact 2.4 Key personnel re notified of necessary training
3. Implement training change	3.1 Training schedule are planned 3.2 Trainings are prioritized and resources are allocated 3.3 Training management plan and procedures are implemented. 3.4 ***High officials*** are involved in the training process 3.5 New performance benchmarks are captured to measure training 3.6 ***Training requirements*** are identified
4. Monitor and review implementation	4.1 Training performance are measured against new benchmarks 4.2 Performance results are submitted to higher officials 4.3 Appropriate documentation and reporting are provided of the training

5. Prepare and deliver training on use of modified system	5.1 Training are prepared to meet the needs of ***client*** in using the changed ***system*** 5.2 Prepared training are delivered appropriate for the client
6. Utilize Specialized Communication Skills	6.1 Specific communication needs of trainees are identified and met. 6.2 Different approaches are used to meet communication needs of the trainees. 6.3 Channels of communication are established and reviewed regularly. 6.4 Communication with trainee is appropriate to individual needs and institutional objectives 6.5 When participating in internal or external forums, presentation is relevant, appropriately researched and presented in a manner to promote the institution 6.6 Utilize appropriate media to enhance presentation. 6.7 Written communication is consistent with institutional standards. 6.8 Strategies which encourage all group members to participate are used routinely. 6.9 Evaluation of group communication strategies is undertaken to promote participation of all parties. 6.10 Effective questioning, listening and nonverbal communication techniques are used to ensure that required message is communicated.

Variable	**Range**
Benchmarks	May include but not limited to: • May include technical, cost savings, performance and quality.
Training needs	May include but not limited to: • May be in reference to the business, system, application, network or people in the organization
Higher officials	May include but not limited to: • end user, internal or external government body, such as team leaders, directors, mangers

Evidence Guide	
Critical aspects of competence	Assessment must confirm the ability to: • plan for, implement, monitor and review change and apply guidelines and policies to the training process • conduct / facilitate users training

Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • Information technology systems • Performance benchmarking • training principles • communication skill • training strategy • multimedia
Underpinning Skills	Demonstrates skills to: • Plan IT training system • Monitor and review implementation
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

NQTF Level III

TOP

Occupational Standard: Hardware and Network Servicing Level III	
Unit Title	**Determine Best-Fit Topology**
Unit Code	**EIS HNS3 01 1221**
Unit Descriptor	This unit defines the competence required to determine the most appropriate way of networking computers to meet user needs and business requirements.

Elements	Performance Criteria
1. Identify key information sources	1.1 Information repositories are identified across the business. 1.2 Current ***organizational documentation*** is reviewed based on business requirements. 1.3 Critical questions are developed to extract information from key stakeholders using a mixture of open and closed questions. 1.4 ***Information gathering techniques*** *are* ensured to use a quality assurance methodology and meet budgetary constraints.
2. Determine user needs	2.1 *Identifying* ***user needs*** *and establishing requirements* 2.2 Different segments are identified for the proposed ***network*** based on business ***requirements.*** 2.3 Segment needs are determined using network functional analysis. 2.4 ***Traffic*** content and volumes are estimated based on business requirements.
3. Develop best topology	3.1 Resource requirements for each network segment are determined on the basis of functional analysis. 3.2 Features of the physical environment are analyzed based on network design. 3.3 Costing process is conducted for possible topology options. 3.4 Appropriate network topology is selected and documented based on business requirements and functional analysis.

Variable	Range
Organizational Documentation	May include business forms, policy documents, financial Statements, performance reports and annual reports.
Information gathering techniques	May include but are not limited to interviews, questionnaires, Surveys and observation.
Network	• May include but is not limited to large and small local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), virtual local area networks (VLANs) and wireless local area networks (WLANs) as well as the use of the public standard telephone network (PSTN) for dial-up modems only, private lines, data and voice • Layer
Requirements	May be in reference to the business, system, application, network or people in the organization
user needs includes:	• Identify user needs • Generate potential solutions • Develop the solutions
Traffic	May include data, voice or video
Types and Sources of Information	• Internet • Virtual library • Organizational policy • Manuals and procedures • Strategic documents • Business requirements • Equipment specifications • Stake holders • Organizational document • Architectural design (blueprint)
Tools and equipment	May include but not limited to: • Toolkit • Connectors • Patch panel • Wall outlet • Cable duct • Network devices (Hubs, Switches, Repeater etc…) • Cables (UTP, STP, Coaxial, Fiber Optics etc…) • Cabinet • Cable tester

Evidence Guide	
Critical aspects of Competence	Assessment must confirm the ability to clearly identify the best LAN, VPN or WLAN topology based on business or organizational needs.

Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • current industry-accepted hardware and software products, including knowledge of general features and capabilities • system's current functionality • characteristics and relative strengths and weaknesses of LAN network topologies • TCP/IP, Ethernet, hubs, adaptor cards • basic knowledge of cabling, particularly UTP (unshielded twisted pair), STP (shielded twisted pair) or optic fiber • network architecture
Underpinning Skills	Demonstrates skills to: • determine user needs • gather data and information • develop best topology for the organization by analyzing user requirements
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level III	
Unit Title	**Install and Manage Network Protocols**
Unit Code	**EIS HNS3 02 1221**
Unit Descriptor	This unit describes the performance outcomes, skills and knowledge required to install and manage network protocols in a networking environment.

Elements	Performance Criteria
1. Install and manage network protocols	1.1 Select, test and validate appropriate network protocol services 1.2 Design a network addressing system, with subnet and host IDs, including appropriate devices 1.3 Configure hosts and workstations to use IP addresses either manually or through automatic allocation of addresses, such as found with dynamic host configuration protocol (DHCP)
2. Identify network protocol applications	2.1 Review a range of well-known network protocol ***applications*** 2.2 Evaluate client user requirement and recommend network-protocol services 2.3 Apply IP addressing scheme according to approved policy and procedures

Variable	Range
Network protocol services may include:	• address resolution protocol (ARP) • DHCP • electronic mail protocols • file transfer protocol (FTP) • H.323 protocol • hypertext transfer protocol (HTTP) • internet protocol (IP) • internet protocol version 4 (IPv4) • internet protocol version 6 (IPv6) • simple network management protocol (SNMP) • simple object access protocol (SOAP) • TCP/IP • wireless application protocol (WAP).
Network may include:	• large and small local area networks (LANs) • virtual private networks (VPNs) • wide area networks (WANs) • Wireless local area networks (WLANs). • Network layering(OSI and TCP/IP)
Devices may include:	• Emulators • gateways • routers.

Applications may include:	• FTP • HTTP • hypertext transfer protocol secure (HTTPS) • secure shell • secure socket layer (SSL) • simple mail transfer protocol (SMTP) • Telnet (not secure).

Evidence Guide	
Critical aspects of competence	Evidence of the ability to: • configure, test and validate network protocols in order to facilitate interconnectivity • install and manage network protocols in a network, and troubleshoot when problems arise.
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • client business domain, including client organisation structure and business functionality • current communications technologies and their associated protocols • current industry-accepted hardware and software products and general features and capabilities • network protocols currently in use in organisation and industry • vendor product range and development directions.

Underpinning Skills	Demonstrates skills to:
	• communication skills to evaluate client user requirements and map to appropriate protocols
	• learning skills to ensure currency with protocols development
	• literacy skills to interpret technical manuals
	• organisational skills to plan, prioritise and organise work
	• problem-solving skills to develop and refine configuration protocols
	• technical skills to:
	  • configure workstations
	  • develop strategic initiatives when designing a network addressing system
	  • test components using available technology
	  • write detailed technical notes.

Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.

Assessment Methods	Competence may be assessed through: • Interview / Written Test Observation / Demonstration with Oral Questioning
Context of Assessment	Competence may be assessed in the work place or in a simulated work place setting.

TOP

Occupational Standard: Hardware and Network Servicing Level III	
Unit Title	**Configure and Administer Server**
Unit Code	**EIS HNS3 03 1221**
Unit Descriptor	This unit defines the competence required to build, configure and test a server

Elements	Performance Criteria
1. Confirm server specification	1.1 ***Network operating system***, ***server applications*** and server design are confirmed with client and system need. 1.2 Product, vendor architecture and ***equipment*** specifications are identified according to the system need. 1.3 Technology and resource are identified within ***business requirements*** and budget.
2. Verify server compatibility and inter-operability	2.1 ***Hardware*** and ***software*** are reviewed to ensure compatibility. 2.2 All hardware required is obtained for ***server*** installation. 2.3 Required ***operating system*** *and* software is Installed for proper function. 2.4 Additional tools or third-party software is installed as required by the created design. 2.5 Operating system and ***applications*** are patched to ensure security and reliability.
3. Configure and test server	3.1 S*erver* is configured as required by ***technical requirements****.* 3.2 Scope and applicability of the testing is defined against technical requirements. 3.3 Test plan is developed with reference to resources and ***network*** impact. 3.4 ***System*** testing is run according to test plan and record outcomes. 3.5 Error report is analyzed and changes are made as required. 3.6 Changes or additions are validated against specifications.

Variable	Range
Network operating system	May include but is not limited to: Novell NetWare 5 or above or operating system that has multi-user ability: Linux 8.0, Mac OSX, and Windows server 2008 or above.

Server applications	May include file sharing, printer sharing, messaging, web services, network and remote access, database and data warehousing, directory services, management, line of business Applications, terminal services.
Equipment	May include but is not limited to: workstations, personal computers, modems and other connectivity devices, printers, DSL modems, hard drives, monitors, switches, hubs, personal digital assistant (PDA) and other peripheral devices.
Business requirements	May be in reference to the business, system, application, network or people in the organization
Hardware	May include but is not limited to workstations, personal computers, modems and other connectivity devices, networks, remote sites, servers.
Software	May include but is not limited to commercial software applications; organization-specific software, packaged software, in-house or customized software
Server	May include: • Application/web servers • DNS and DHCP servers • Email servers • File and print servers • FTP servers • Firewall servers • Proxy/cache server
Operating system	May include but is not limited to Linux 8.0 or above, Windows 2008/Server 2012 or above, Apple OS X or above.
Application	May include database programs, word processors, email programs, internet browsers, system browsers and spreadsheets.
Technical requirements	May be in reference to the business, system, platform, application, database, network or people in the organization.
Network	May include but not limited to large and small LANs, national WANs, the internet, the use of the PSTN for dial-up modems only, private lines, data and voice.
System	May include but is not limited to databases, applications, servers, operating systems, gateways, application service provider and ISP.

Evidence Guide	
Critical aspects of competence	Assessment must confirm the ability to administer, configure and test a server according to business needs and technical requirements.

Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • Single and multiple processors, memory, Disk drives and internal/external storage devices. • Server applications (such as web application, DNS, etc.) • Server specification for different applications
Underpinning Skills	Demonstrates skills to: • determine server specifications • determine compatibility and operability • configured a server as required by technical requirements
Resources Implication	• Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	• Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: **Hardware and Network Servicing Level III**	
Unit Title	**Monitor and Administer System and Network Security**
Unit Code	**EIS HNS3 04 1221**
Unit Descriptor	This unit defines the competence required to monitor and administer security functions of a system.

Elements	**Performance Criteria**
1. Ensure user accounts are controlled	1.1 Default ***user*** settings are modified to ensure that they conform to ***security policy.*** 1.2 Previously created user settings are modified to ensure they conform to updated security policy***.*** 1.3 Legal notices are displayed ensured at logon are appropriate. 1.4 Appropriate utilities are used to check strength of passwords and consider tightening rules for password complexity. 1.5 Action taken to ensure password procedures are reviewed with appropriates other internal departments. 1.6 Information services are accessed to identify security gaps and appropriate action taken using ***hardware*** and ***software*** or patches.
2. Secure file and resource access	2.1 Inbuilt security and access features of the ***operating system*** are reviewed and considered for further action 2.2 File security categorization scheme, and an understanding of the role of users is developed or reviewed in setting security. 2.3 Virus checking process is implemented and scheduled for the ***server***, computer and other system components.
3. Determine authentication requirements	3.1 User and enterprise security requirements are determined with reference to enterprise security plan. 3.2 Authentication options are identified and analyzed according to user and enterprise requirements. 3.3 Most appropriate authentication and authorization processes are selected based on security requirements.
4. Determine network security	4.1 Users shared resources access via a network with reference to enterprise security plan 4.2 ***Security threats*** are monitored and recorded to the system. 4.3 The latest antivirus signatures are updated.

Variable	Range
Security policy	May be in relation to theft, viruses, standards (including archival, back-up, network), privacy, audits and alerts; usually relates directly to the security objectives of the organization.
Hardware	May include but is not limited to workstations, personal computers, modems or other connectivity devices, networks, DSL modems, remote sites, servers.
Software	May include but is not limited to commercial, in-house, packaged or customized software.
Operating system	May include but is not limited to Linux 6.0 or above, Windows 7 or above, Apple OS 8 or above.
Server	May include: • Application/web servers • BEA Web logic servers • IBM Visual Age and Web Sphere • Novell NDS servers • Email servers • File and print servers • FTP servers • Firewall servers • Proxy/cache servers
Security threats	May include eavesdropping, manipulation, impersonation, penetration, denial of service, by-pass, hacking, viruses.

Evidence Guide	
Critical aspects of competence	Assessment must confirm knowledge of the security features available in the operating environment and the ability to monitor and administer security functions on the network.
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • client business domain, business function and organization • features and capabilities of networking technologies, with substantial depth in security areas • network and system security
Underpinning Skills	Demonstrates skills to: • secure file and resource access • determine authentication requirements and network security
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level III	
Unit Title	**Identify and Resolve Network Problems**
Unit Code	**EIS HNS3 05 1221**
Unit Descriptor	This unit defines the competence required to troubleshoot local area network problems.

Elements	Performance Criteria
1. Implement regular network monitoring	1.1 An appropriate log is set up to monitor network activity and to produce a management information base (MIB). 1.2 ***Network tools*** are used to benchmark the ***network*** and to establish a reference point for network performance. 1.3 Documents and logs regularly reviewed to facilitate network tuning. 1.4 Recommendations are made to management for additional network resources to improve performance or to pro-actively avoid problem.
2. Troubleshoot network problems	2.1 Help desk and other support services are addressed to quickly identify network problems. 2.2 Various tools and knowledge of ***network topology*** and protocols are used to identify and solve network problems. 2.3 ***Users*** and clients of progress and solutions are advised in a timely manner. 2.4 Support ***documentation*** is completed based organizational requirement.
3. Carry out maintenance support on identified problem	3.1 Diagnostic tests around identified problem are conducted based on requirement. 3.2 Maintenance is completed in line with ***organizational guidelines.*** 3.3 New ***components*** as part of the resolution are obtained where necessary. 3.4 Components are stored or dispose in accordance with organizational guidelines***.***

Variable	Range
Network tools	May include but are not limited to Snort, Satan Saint, Netbus, Ping, Netstat, Nmap, traceroute, Whois, Dig etc...
Network	May include but is not limited to large and small LANs, VPNs, WANs, the internet, the use of the PSTN for dial-up modems only, private lines, data and voice.
Network topology	May include ring, star, bus, hierarchical and hybrid
User	May include a person within a department, a department within the organization or a third party.
Documentation	May follow ISO/IEC/AS standards, audit trails, naming standards, version control, project management templates and report writing principles.
Organization guidelines	May include but are not limited to security procedures; logged call procedures; client liaison policy; preventative maintenance and diagnostic policy; maintenance agreements; warranties; contracting arrangements relating to IT purchasing.
Components	May include motherboards, CMOS battery, central processing unit (CPU), CD and DVD drives, interface cards, drives, fax/modem cards, RAM upgrades, CPU upgrades.

Evidence Guide	
Critical aspects of competence	Assessment requires evidence that the candidate: • troubleshoot and monitored facilities available in the operating environment • undertaken logical troubleshooting processes and network support activities • performed constant monitoring of the network to maintain network activities • performed network maintenance with minimal disruption to clients
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • current industry-accepted hardware and software products, with knowledge of general features and capabilities • networking technologies (e.g., TCP/IP, OSI protocol stacks) with knowledge of features and capabilities, and substantial depth in protocols such as Ethernet, AppleTalk, Novell, Linux or UNIX protocols • network management tools, with knowledge of general features and capabilities, with substantial depth in troubleshooting areas
Underpinning Skills	Demonstrates skills to: • perform regular monitoring

	• solve network related problems • perform maintenance support
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level III	
Unit Title	**Provide First Level Remote Help Desk**
Unit Code	**EIS HNS3 06 1221**
Unit Descriptor	This unit defines the competence required to provide advice and support to clients including the communication of comprehensive technical information.

Elements	Performance Criteria
1. Analyze client support issues	1.1 New problems logged by ***client*** are checked 1.2 Previous logs for similar problems or requests from client are checked 1.3 Support issues affecting the client are investigated and documented 1.4 Client of the results of ***investigation*** and provide ***advice*** and ***support*** on findings are notified 1.5 Client feedback and make changes are obtained
2. Provide advice on software, hardware or network	2.1 Software, hardware or network requirements with clients are confirmed 2.2 Solution for the hardware and software problems are investigated and documented 2.3 Additional requirements discovered in the investigation and refer them to the clients are documented 2.4 Approval from the client to implement the solutions are obtained 2.5 Amount of technical support the client may require are investigated and documented 2.6 Level of technical support identified with the client are discussed and agreed 2.7 Time with the client when support will take place is arranged 2.8 Technical support as part of group or one-to-one instruction to the client is provided 2.9 Manuals and help ***documentation*** to the clients are provided

3. Obtain client feedback	3.1 An appropriate evaluation or feedback form or other mechanism to gather feedback about the solution and support provided are created. 3.2 Client with instructions on how to complete the form or use other means of providing feedback is provided. 3.3 Evaluation or feedback to the client is distributed. 3.4 Feedback from the client to identify areas for improvement is reviewed.
4. Lead Workplace Communication	4.1 Appropriate communication method is selected based on work place guideline. 4.2 Constructive contributions are made to workplace discussions on such issues as production, quality and safety. 4.3 Information regarding problems and issues are organized coherently to ensure clear and effective communication. 4.4 Communication problems and issues are raised as they arise.

Variable	**Range**
Client	May include but not limited to: • internal departments, external organizations, individual people and employees
Investigation	May include but not limited to: • on-site examination; questions and answers; active listening to clients and colleagues; contacting vendor or maintenance organizations; reviewing technical advice about the organization
Advice and support	May include but not limited to: • provision of client documentation, manuals; one-to-one training; identification of training need for referral to supervisor; documentation from vendor; advice on software supported by the organization, • use of macros, statistical functions of spreadsheets, creation of templates, generation of a complex report on a database, password and log-on procedure; • advice on hardware supported by the organization, including but not limited to printers, laptops, notebooks, CD-ROM, screens, disk drives, reconfiguration of settings, operation of scanners
Solution	May include but not limited to: • new hardware, hardware upgrades, new software, software upgrades, user training and implementing a new system
Documentation	May include but not limited to:

	• a collection of records that describe the structure, purpose, operation, maintenance and data requirements for a computer program, operating system or hardware device

Evidence Guide	
Critical aspects of competence	Assessment must confirm the ability to: • convey comprehensive technical information to clients in a clear, concise and coherent manner • access technical manuals and help documentation and to convey this information to the client in a concise and jargon-free manner • Convey information to enhance client efficiency
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • Operating systems supported by the organization • Advanced features and functions of software • Information sources • Contract and service agreements with vendors • Operating systems functions and basic features • Hardware and software supported by the organization • Features of different types of hardware • Security and network guidelines and procedures • Available in-house and vendor support
Underpinning Skills	Demonstrates skills to: • analyze support issues • conduct investigation • provide advice on software, hardware or network
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level III	
Unit Title	**Create Technical Documentation**
Unit Code	**EIS HNS3 07 1221**
Unit Descriptor	This unit defines the competence required to create technical documentation that is clear to the target audience and easy to navigate.

Elements	Performance Criteria
1. Identify and analyze documentation needs	1.1 ***Client*** is consulted to identify documentation ***requirements*** 1.2 Documentation requirements are interpreted and evaluated, and details with the client confirmed 1.3 Industry and ***documentation standards*** are investigated for requirements 1.4 Scope of work is defined and documented to be produced 1.5 Client is consulted to validate and confirm the scope of work
2. Design documentation	2.1 Information requirements are identified with reference to layout and structure documented 2.2 Document templates and style guides are created consistent with information requirements 2.3 Review of the ***system*** is conducted in order to understand its functionality 2.4 Content that meets information requirements is extracted in accordance with relevant copyright restrictions 2.5 Structure of the ***technical documentation*** is developed giving focus to the flow of information, style, tone and content format 2.6 Technical documentation structure is validated with the client
3. Develop documentation	3.1 Technical documentation is written based on the template and scope of work using the information gathered 3.2 Technical terminology is translated into plain English where appropriated 3.3 ***Content*** format and style is applied in accordance with relevant documentation standards and templates
4. Evaluate and edit documentation	4.1 Technical documentation is submitted to ***appropriate person*** for reviewed 4.2 Feedback is gathered and analyzed

	4.3 Alterations into the technical documentation is incorporated 4.4 Technical documentation is edited for technical and grammatical accuracy

Variable	Range
Client	May include but is not limited to internal departments, external organizations, individual people and internal employees
Requirements	May be in reference to the business, system, application, organizational policies, network or people in the organisation
Documentation standards	May include but are not limited to policy relating to sign-off, storage, distribution, revision. May include ISO/IEC/AS standards, organizational standards, audit trails, naming conventions, version control, project management templates and report writing principles
System	May include but is not limited to network, application, software, business, computers, financial system, management system and information system
Technical documentation	May include system or project specifications, system design, system functionality, reports, help references, technical manuals, operational procedures, training materials and self-paced tutorials, on-line help, user guides and brochures.
Content	May include information and interactive features, such as product information, company information, copyright and disclaimer notices, site map, frequently asked questions, what's new, customer-specific information, customer only information, error messages, instructions, feedback mechanisms, reference pages, forms, background articles, ratings/rankings/testimonials/quotes from reviews, hyperlink titles.
Appropriate person	May include a supervisor, teacher, authorized business representative or client.
Channels	May include text, audio, animation and graphics provided through books, manuals, CD-ROMs, DVDs, computer-based tutorials, help screens and the world wide web.

Evidence Guide	
Critical aspects of competence	Assessment must confirm the ability to create technical documentation that meets business requirements, caters for a diverse readership, is clear to the target audience and easy to navigate such as • identified and analyzed documentation needs • designed documentation

	• developed documentation • evaluated and edited documentation
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • content features, such as clarity and readability • instructional design principles • functions and features of templates and style guides • document design, web design and usability • the use of word processing software and multimedia authoring tools • identifying target audiences • analyzing audience needs • identifying relevant content • determining appropriate content, formats and styles • writing content
Underpinning Skills	Demonstrates skills to: • design documentation • develop documentation • evaluate and edit documentation
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

NQTF Level II

TOP

Occupational Standard: Hardware and Network Servicing II	
Unit Title	**Operate Database Application**
Unit Code	**EIS HNS2 01 1221**
Unit Descriptor	This unit defines the competency required to operate database applications and perform basic operations.

Elements	Performance Criteria
1. Create database objects	1.1 Database application is opened and designed incorporating basic ***design principles*** 1.2 Database object is created according to database usage, as well as user requirements 1.3 Database object is modified as required 1.4 Data in a table are added and modified according to information requirements 1.5 Records are added, modified and deleted as required 1.6 Database objects are saved and compiled
2. Customize basic settings	2.1 ***Page layout*** is adjusted to meet user requirements 2.2 Different ***toolbars*** are opened and viewed 2.3 ***Font*** is *formatted* as appropriate for the purpose of the database entries
3. Create forms	3.1. Wizard used to create a simple form 3.2. Existing database opened and records through a simple form modified 3.3. ***Objects*** within the form rearranged to accommodate information requirements
4. Retrieve information	4.1 Existing database is accessed and required records located 4.2 Simple query is created and required information retrieved 4.3 Query with multiple criteria is developed and required information retrieved 4.4 Data are selected and appropriately displayed
5. Create reports	5.1 Reports are designed to present data in a logical sequence or manner 5.2 Reports are modified to include/exclude additional requirements

	5.3 Reports are distributed to ***appropriate person*** in approved format

Variable	**Range**
Occupational Health & Safety (OH&S)	• Correct posture, lighting, and type of desk, type of monitor, style of chair, typing position, repetitive strain injury prevention, ventilation, light position, correct lifting method, and length of time in front of computer. • May also include physical safety considerations such as general electrical safety and cabling, power supply and leads as they apply to computer and peripheral installations.
Design principles	May include • naming conventions • data layout • formatting
Page layout	May include • landscape • portrait
Toolbars	May can contain • buttons • menus or a combination of both
Font	May include • The combination of typeface and other attributes, such as size, pitch, and spacing character or symbol.
Appropriate person	May include • a supervisor • teacher • authorized business representative or client
Objects	May include • buttons • checkboxes • option buttons • text boxes • drop down lists
Tools and equipment	May include but not limited to: • Computers, DB applications, DBMS

Evidence Guide	
Critical Aspects of Competence	Assessment must ensure candidate has the ability – • to design and develop a simple database using a standard database package • to add data, use queries, and create forms and reports • create and format documents • customize basic settings to meet page layout conventions
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • basic database design • basic settings and context • relationships between tables (cardinality) • forms, reports and queries for retrieving and displaying information
Underpinning Skills	Demonstrates skills to: • create database objects • customize basic settings • retrieve information
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: **Hardware and Network Servicing II**	
Unit Title	**Install and Optimizes Operating system Software**
Unit Code	**EIS HNS2 02 1221**
Unit Descriptor	This unit defines the competence required to install operating system (OS) software and to make adjustments as a means of optimizing the system to accommodate business and client needs clearly

Elements	Performance Criteria
1. Determine function of operating system	1.1 Identify and demonstrate understanding of ***operating system*** purposes 1.2 Distinguish between batch system, real-time system, multi-tasking system 1.3 Compare and contrast different operating systems and their features 1.4 Identify and demonstrate the knowledge of basic operating system functions, including file system, memory management, process scheduling 1.5 Identify and demonstrate management of virtual memory
2. Obtain operating system	2.1 Contact operating system vendors to obtain technical specifications and system requirements 2.2 Identify the process and steps required to install and configure the operating system using ***installation components*** 2.3 Document adjustment recommendations and provide to ***appropriate person*** 2.4 Determine and apply knowledge of licensing, hardware and security requirements
3. Install, configure and optimize operating system	3.1 Install, configure and test operating system using installation components and ***boot-utility options*** 3.2 Use the relevant ***operating system user interface*** to correctly configure the installation 3.3 Optimise the system to meet ***organisational requirements*** 3.4 Document the system according to organisational requirements 3.5 Install the operating system with minimal disruption to ***client*** or users

4. Provide instruction to meet new software requirements	4.1 Provide one-to-one instruction about changes to the client or users as required 4.2 Obtain client evaluation about new system to ensure requirements are met, using appropriate ***feedback mechanism***

Variable	**Range**
Operating system may include:	• Microsoft Windows: • Windows Vista (32 bit versus 64 bit) • Windows 7 (32 bit versus 64 bit) and above

Installation components may include:	• configure power management:
	  • hibernate
	  • sleep timers
	  • standby
	• demonstrate safe removal of peripherals
	• device manager:
	  • driver signing
	  • install and update devices drivers
	  • verify
	• directory structures:
	  • create folders
	  • navigate directory structures
	• disk preparation order:
	  • Dual installation
	  • format drive
	  • partition
	  • start installation
	• files:
	  • attributes
	  • creation
	  • extensions
	  • permissions
	• file systems, such as FAT32 versus new technology file system (NTFS)
	• installation methods:
	  • boot media, such as DVD, CD, universal serial bus (USB)
	  • factory recovery partition
	  • install from image
	  • network installation
	  • recover CD
	• operating system installation options:
	  • file system type
	  • network configuration
	  • repair installs
	• user data migration - user state migration tool (USMT)
	• verification of hardware compatibility and minimum requirements
	• Virtual memory

Appropriate person may include:	• authorised business representative • client • Supervisor

Boot-utility options may include:	• automated system recovery (ASR) • boot options • boot to restore point • disk boot order or device priority • emergency repair disk (ERD) • recovery console • recovery options • safe mode • Types of boot devices (disk, network, USB).

Operating system user interface may include:	• Windows-adopting interface to undertake similar tasks with chosen operating system:
	  • administrative tools, such as performance monitor, event viewer, services and computer management
	  • command prompt utilities, such as ipconfig, Ping and Telnet
	  • control panel
	  • location of basic network settings between OS versions
	  • MMC
	  • my computer
	  • my network places or home group
	  • run line utilities:
	  • *cmd*
	  • *direct diagnostics (DXdiag)*
	  • *msconfig*
	  • *MSINFO32*
	  • *REGEDIT*
	  • start menu
	  • task bar
	  • task manager
	• Windows Explorer - Libraries in Windows 7.

Organizational requirements may include:	• availability of system to be optimised • client support documentation • in-house or vendor • contracting arrangements relating to IT purchasing • IT policy and procedures relating to service levels and installation level of complexity of technical manuals.
Client may include:	• department within the organisation • person with special needs • Person within a department third party.
Feedback mechanism may include:	• Interview • meeting • Questionnaire survey.

Evidence Guide	
Critical Aspects of Competence	Demonstrates a knowledge and skills of: • Install, configure and test an operating system to improve system performance with minimum disruption to clients.
Required Knowledge and Attitudes	Demonstrates knowledge of: • current industry-accepted hardware and software products • functions and features of operating systems used by the organisation • installation and configuration of systems software • architecture of current technical systems • deployment of current organisational systems • organisational requirements for operating system software • prerequisites for system software installation • set-up and configuration procedures • software packages supported by the organisation • system's current functionality • system's diagnostic software • Vendor specifications and requirements for installation.
Required Skills	Demonstrates skills to: • liaise with people working across different levels and in different contexts, such as operating system vendors and clients • literacy skills • interpret technical computer installation manuals • obtain written and verbal feedback from clients • present information, such as the use of diagnostic tools • provide verbal instructions to client technical skills • install and configure operating system software • Write instructions for clients
Resource Implications	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices
Methods of Assessment	Competence may be assessed through • Interview / Written Test • Observation / Demonstration with Oral Questioning
Context of Assessment	Competence may be assessed in the work place or in a simulated work place setting.

TOP

Occupational Standard: Hardware and Network Servicing II	
Unit Title	**Administrate Network and Hardware Peripherals**
Unit Code	**EIS HNS2 03 1221**
Unit Descriptor	This unit defines the competence required to connect, install, configure, maintain and troubleshoot local area network and peripherals

Elements	Performance Criteria
1. Confirm requirements of client	1.1 ***Client peripheral*** requirements are Identified and confirmed in accordance with ***organizational standards***. 1.2 Client requirements and peripherals needed are documented in line with organizational standards and report findings to the ***appropriate person.*** 1.3 Client requirements are verified with appropriate person in line with organizational standards and reporting procedures. 1.4 Action taken to ensure client support expectations are covered by vendor warranty and support services.
2. Obtain required peripherals	2.1 Peripherals are obtained under instruction from appropriate person. 2.2 Peripherals are entered into ***equipment*** inventory according to organizational standards. 2.3 Contents of delivered components and physical contents that match the packing list are validated and resolved discrepancies if necessary. 2.4 Peripherals are stored according to vendor/manual guidelines.
3. Connect hardware peripherals	3.1 Timeframe for installation schedule is verified with the client requirement. 3.2 Old peripherals are removed if they are being replaced with minimal disruption to clients, taking into account ***environmental considerations*** and ***OHS standards***. 3.3 New peripherals are connected with minimum disruption to *clients*, taking into account ***operating system*** procedures. 3.4 The computer configured to accept the new peripherals based on business requirement 3.5 Hardware peripherals are tested and confirmed to client satisfaction, pay particular attention to possible impact on other systems and make adjustments as required.

4. Install and Configure peripherals to a network	4.1 Location of peripherals are planned to provide appropriate services to ***users*** and to take into consideration OHS standards. 4.2 Peripherals are connected to ***network***, using vendor-approved method and technology. 4.3 Peripherals are connected to computers in the network using parallel, serial or other direct connection methods appropriate for the job order. 4.4 Peripherals are tested for correct operation based on client's specifications. 4.5 Required ***software*** is installed to manage local and network-connected peripherals according to business requirement software peripherals according to business requirement. 4.6 Meaningful names are used for peripherals and control queues 4.7 Security and access are configured to allow appropriate users to make use of peripherals. 4.8 Workstation for peripherals is configured to allow ***applications*** to work with peripherals.
5. Administer and support peripheral services	5.1 Priority is assigned to control queues based on organizational requirement. 5.2 Settings on the network is configured to create maintenance schedules, usage logs, and cost center usage statistics 5.3 Methods are demonstrated to the user for using peripheral services from their application or workstation
6. Use command line tools	6.1 Outline command-line environment 6.2 Differentiate command-line and graphical user interface (GUI) system 6.3 List ***command-line tools*** 6.4 Apply command-line tools in ***GUI environment***
7. Maintain peripherals and fix common problems	7.1 A regular maintenance schedule is established and followed as recommended by peripheral manufacturer. 7.2 ***Consumables*** and components are replaced when required. 7.3 Peripheral mishaps (unfortunate accident) and malfunctions are fixed based on procedure.

	7.4 Peripheral usage and traffic is monitored and recommend additional peripherals if needed. 7.5 Failures of peripheral services or devices are determined and rectify as required.
8. Use and maximize operating system	8.1 Operating system is configured to suit the working environment, including but not limited to setting variables. 8.2 Application software is installed, upgraded and uninstalled to suit the working environment. 8.3 Both graphical user interface and the command line interface are used to perform basic tasks based on clients. 8.4 Operating system and third-party utilities are used based system requirement. 8.5 Graphical user interface is customized based on clients.
9. Support input and output devices	9.1 Input and output devices are set up and checked functionality based on requirement. 9.2 Drivers are installed as appropriate and checked functionality-based vendor manuals. 9.3 Drivers are ensured to be properly working

Variable	**Range**
Client	May include but is not limited to internal departments, external organizations, individual people and employees
Peripherals	• May include but are not limited to**:** • Printers, scanners, tape cartridges • Speakers, multimedia kits • Personal computer, modems • Input equipment may include mouse, touch pad, keyboard,
Organizational Standards	May include but are not limited to personal use of emails and internet access, content of emails, downloading information and accessing particular websites, opening mail with attachments, virus risk (MS windows OS and Mac OS only), dispute resolution, document procedures and templates, communication methods and financial control mechanisms
Appropriate person	May include a supervisor, teacher, authorized business representative or client
Equipment	May include but is not limited to workstations, personal computers, modems or other connectivity devices, printers, hard drives, monitors, switches, hubs, personal digital assistant (PDA) and other peripheral devices OH&S standards May include correct posture, lighting, type of desk, type of monitor,

	style of chair, typing position, repetitive strain injury prevention, ventilation, light position, correct lifting method, and length of time in front of computer.
Environmental considerations	May include disposal of packaging (e.g. cardboard, polystyrene, paper, plastic) and redundant hardware (e.g. hard drives, circuit boards).
Occupational Health and Safety (OHS)	OHS precautions and measures may include against: • Physical hazards – impact, illumination, pressure, noise, vibration, temperature, radiation • Chemical hazards – dusts, fibers, mists, fumes, smoke, gasses, vapors • Ergonomics • Psychological factors – over exertion/ excessive force, awkward/static positions, fatigue, direct pressure, varying metabolic cycles • Physiological factors – monotony, personal relationship, work out cycle • Burglary • Fire • Power accidents
Operating system	May include Win7 and above, Sun Solaris/SunOS, HP-UX, AIX, Silicon Graphics IRIX, DEC VMS, Mac OS X, Linux, NetWare
User	May include a person within a department, a department within the organization or a third party
Network	May include but is not limited to large and small LANs, WANs, VPNs, the internet, the use of the PSTN for dial-up modems only, private lines, data and voice.
Software	May include but is not limited to commercial, in-house, packaged or customized software
Applications	May include database programs, word processors, email programs, internet browsers, system browsers and spreadsheets
Consumables	May include but is not limited to ink cartridges, toner cartridges, ribbons, floppy disks, CD-RW
Network operating system	May include but is not limited to Novell NetWare 5 or above or any operating system that has multi-user ability, Linux, Mac OS, Windows 7 or above.
Tools and Equipment	• Hardware peripherals and workstation • Live network • Cables • Network operating system • Soft wares • Toolkit • Cable tester • Printer (laser printers and ink jet printers[mono or colored])

Command line tools may include:	• Ping Localhost (127.0.0.1) • Ipconfig • Ipconfig/all • Ping
GUI environment may include but not limited to:	• Windows platforms.

Evidence Guide	
Critical aspects of competence	Assessment must confirm knowledge of • peripheral technologies and how network peripherals (hardware and software) are installed and configured • ability to maintain networked peripherals in working order • ability to safely connect hardware peripherals according to vendor instructions with a minimum of down time to the system
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • current peripheral devices, such as scanners, multi-use devices, external modems • how to configure peripherals for network use, with drivers and cable connections • organizational guidelines relating to external suppliers and vendors • general understanding of technical systems • general knowledge of operating systems • general knowledge of help desk and maintenance practices • current industry-accepted hardware and software products • broad knowledge of input/output devices
Underpinning Skills	Demonstrates skills to: • connect hardware peripherals • use operating system • configure peripheral Services to manage peripherals
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing II	
Unit Title	**Implement Maintenance Procedures**
Unit Code	**EIS HNS2 04 1221**
Unit Descriptor	This unit defines the competence required to set up maintenance procedures to keep equipment and software operating effectively and efficiently.

Elements	Performance Criteria
1. Determine best practices for equipment and software maintenance	1.1 ***Equipment*** and ***software*** to be maintained and implemented processes are identified to ensure future acquisitions of equipment and software. 1.2 Vendor ***documentation***, peer organizations or research information detailing best practices in equipment and software maintenance are identified to improve system performance and reliability. 1.3 ***Requirements*** are obtained from user in the area of equipment maintenance and reliability. 1.4 Procedures are documented for maintenance based upon best practices.
2. Revise practices, where appropriate	2.1 Maintenance operation is monitored and reviewed where appropriate. 2.2 Problem areas including failures are identified to meet ***service-level agreements***, and consider changes to maintenance procedures. 2.3 Changes are assessed in consultation with user, support staff and third party suppliers. 2.4 Improvements are designed and implemented to maintenance procedures.
3. Identify and analyze IT system components to be maintained	3.1 Warranty status of components and/or software is determined and documented according to vendor, project or organizational requirements. 3.2 ***System architecture*** and configuration documentation are reviewed for currency status. 3.3 Critical components and/or software are identified and recommendations are documented regarding possible service arrangements.
4. Apply maintenance procedures	4.1 Preventative maintenance schedule is created based on cost, business and service-level agreements requirements

	4.2 Specific and appropriate maintenance procedure is identified and applied based on cost, business and service-level agreements requirements 4.3 Recommended procedures are documented and submitted for approval in accordance with organizational requirements and service-level agreement 4.4 Implementing staff are oriented on the procedures and ensured to follow the maintenance schedule 4.5 ***OHS*** is observed throughout the process

Variable	**Range**
Equipment	May include but is not limited to workstations, personal computers, modems and other connectivity devices, printers, DSL modems, hard drives, monitors, switches, hubs, personal digital assistants and other peripheral devices
Software	May include but is not limited to commercial, in-house, packaged or customized software
Documentation	May follow ISO/IEC/AS standards, audit trails, naming standards, version control, project management templates and report writing, maintaining equipment inventory; client training and satisfaction reports
Requirements	May be in reference to the business, system, application, network or people in the organization
Service-level agreement	May exist for many different infrastructure services, including communications carriers, ISPs, ASPs and SLAs for vendor products, workload and performance considerations, expectations regarding servicing, penalties, and charge back to business units.
Systems architecture	May include but not limited to: • Operating system: Novell NetWare 5 or above or operating system that has multi-user ability, Linux, Mac OS, Windows 7 or above • Database software: Oracle, Sybase, Microsoft SQL server, Ingres, DB2, Informix, MSQL, MySQL, SQL server • Configuration: small memory model, large memory model, requests per second
Tools	• Hardware and Software • Blower • Cleaning agents(alcohol, contact cleaner) • Tool kit • Maintenance Safety tools • Multi meter

Occupational Health and Safety (OHS)	OHS precautions and measures may include against: • Physical hazards – impact, illumination, pressure, noise, vibration, temperature, radiation • Chemical hazards – dusts, fibers, mists, fumes, smoke, gasses, vapors • Ergonomics ▪ Psychological factors – over exertion/ excessive force, awkward/static positions, fatigue, direct pressure, varying metabolic cycles ▪ Physiological factors – monotony, personal relationship, work out cycle • Burglary, Fire and Power accidents

Evidence Guide	
Critical Aspects of Competence	Assessment must confirm ability to- • determine the best practice for hardware and software maintenance • set up efficient and responsive maintenance procedures to keep equipment and software operating
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • client business domain • current industry-standard hardware and software products and its features • equipment and software maintenance • safety procedures and practices in computer maintenance • techniques and procedure in determining system's current functionality • system performance and maintenance procedures • operation and use of diagnostic tools
Underpinning Skills	Demonstrates skills to: • identify and analyze maintenance needs • analyze IT system components to be maintained • determine and apply best practices for equipment and software maintenance • use diagnostic tools
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing II	
Unit Title	**Maintain Equipment and Consumables**
Unit Code	**EIS HNS2 05 1221**
Unit Descriptor	This unit defines the competence required to maintain the operation of basic computer hardware and peripherals including the replacement of consumables.

Elements	Performance Criteria
1. Clean equipment	1.1 Cleaning supplies are accessed and verified for usability on the selected equipment 1.2 Maintenance actions undertaken are recorded and documented according to organizational procedures 1.3 Equipment's *are* cleaned as per manufacturer specifications and in line with organizational manuals
2. Replace and maintain consumables and supplies	2.1 Access ***consumables*** from storage points and record usage information in line with organizational procedures 2.2 Replace consumables when needed and log the action undertaken 2.3 Dispose of consumables following environmental guidelines 2.4 Test equipment to ensure it is in working order at set time periods and in line with organizational procedures
3. Maintain equipment	3.1 Equipment are identified which requires maintenance 3.2 Equipment *is* maintained as required by organizational guidelines and manufacturer specifications. 3.3 Maintenance procedures are documented as required by organizational guidelines. 3.4 Care is exercised to prevent interruption of business activities during maintenance procedures 3.5 Unused equipment devices are stored in line with manufacturer specifications and organizational guidelines

Variable	Range
Tools and Equipment	• Hardware and Software • Blower • Cleaning agents(alcohol, contact cleaner) • Toolkit • Static wrist strap • Multi meter
Consumables	May include disks, ribbons, printer toner, paper, cartridges, cleaners and tape

Equipment	May include but is not limited to workstations, personal computers, modems and other connectivity devices, printers, hard drives, monitors, DSL modems, switches, hubs, and other peripheral devices
Occupational Health and Safety (OHS)	OHS precautions and measures may include against: • Physical hazards – impact, illumination, pressure, noise, vibration, temperature, radiation • Chemical hazards – dusts, fibers, mists, fumes, smoke, gasses, vapors • Ergonomics ▪ Psychological factors – over exertion/ excessive force, awkward/static positions, fatigue, direct pressure, varying metabolic cycles ▪ Physiological factors – monotony, personal relationship, work out cycle • Burglary, Fire and Power accidents • Environmental guidelines - recycling, safe disposal of packaging (e.g. cardboard, polystyrene, paper, plastic) and correct disposal of redundant hardware (e.g. motherboards, hard drives, circuit boards) by an authorized body

Evidence Guide	
Critical Aspects of Competence	Assessment must confirm the ability to maintain equipment in working order and to replace equipment and consumables.
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • OHS principles and concept • Equipment and consumables uses and characteristics • Maintenance procedures and techniques • Chemical storage, control and disposal • Basic understanding of organizational systems, in relation to storage and retrieval of information and equipment • Basic knowledge of current industry-accepted hardware and software and manufacturer maintenance guides
Underpinning Skills	Demonstrates skills to: • clean equipment • maintain equipment • interpreting manufacturer’s instructions • writing maintenance reports
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration

Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing II	
Unit Title	**Connect Internal Hardware Component**
Unit Code	**EIS HNS2 06 1221**
Unit Descriptor	This unit describes the performance outcomes, skills and knowledge required to modify and connect system hardware components according to client and user requirements.

Elements	Performance Criteria
1. Identify, categorize and distinguish the different types of internal hardware components	1.1 Identify and categorise the different ***internal hardware components*** 1.2 Explain and Distinguish the purpose and characteristics of the different internal hardware component categories
2. Determine components required	2.1 Identify and clarify user internal hardware component requirements according to ***organisational guidelines*** 2.2 Organize and record user component requirements, pass on to ***appropriate person*** for evaluation and vendor selection
3. Obtain components	3.1 Contact vendors to obtain technical specifications for the proposed components 3.2 Assess the options and provide recommendations to the appropriate person for final analysis 3.3 Obtain components to prepare for installation
4.Install components	4.1 Develop plans, with prioritised tasks and contingency arrangements, for the installation of selected components with minimum disruption to ***clients*** 4.2 Liaise with appropriate person to obtain approval for the plans 4.3 Install and configure components according to plan, installation procedures and ***organisational requirements*** 4.4 Test components for error-free performance, using available technology 4.5 Identify and resolve identified problems 4.6 Test and enhance system performance, using knowledge of the system, to meet organisational benchmarks 4.7 Document the installation and configuration process according to organisation guidelines

5. Evaluate modified system	5.1 Collect client or user feedback and analyse against client requirements 5.2 Correct identified shortcomings in the system and record actions

Variable	**Range**
Internal hardware components may include:	• adapter card components: • communications: • modem • network interface card (NIC) • I/O: • Parallel port • small computer system interface (SCSI) • serial port • universal serial bus (USB) • multimedia: • capture cards • sound card • TV tuner cards • video: • AGP • peripheral component interconnect (PCI) • PCIe • cooling system components: • CPU and case fans • heat sinks • liquid cooling systems • thermal compound • CPU components and features: • 32 bit versus 64 bit • hyper threading • identify CPU types: • AMD • Intel • multi-core: • dual core • quad core • triple core • onchip cache: • L1 • L2 • speed (real versus actual) • display device components: • connector types:

	• component or RGB • DVI pin compatibility • HDMI • S-Video • VGA • LCD technologies: • contrast ratio • native resolution • resolution (e.g., XGA, SXGA+, UXGA, WUXGA) • projectors, CRT and LCD • settings: • degauss • multi-monitor • refresh rate • resolution • memory components and features: • ECC versus non-ECC • parity versus non-parity • single channel versus dual channel • single sided versus double-sided • speed: • PC100 • PC133 • PC2700 • PC3200 • DDR3-1600 • DDR2-667 • types: • DRAM • SRAM • SDRAM • DDR or DDR2 or DDR3 • RAMBUS • motherboard components: • basic input/output system (BIOS), complementary metal oxide semiconductor (CMOS) or Firmware: • CMOS battery • POST • bus architecture • bus slots: • AGP • AMR • CNR • PCI • PCIe

	• Personal Computer Memory Card International Association (PCMCIA) • chipsets • contrast RAID (levels 0, 1, 5) • form factor: • ATX or BTX • micro ATX • NLX • I/O interfaces: • IEEE 1394 or Firewire • modem • NIC • parallel • PS/2 • serial • sound • USB 1.1 and 2.0 • video • memory slots: • DIMM • RIMM • SIMM • SODIMM • parallel advanced technology attachment (PATA): • EIDE • IDE • processor sockets • riser card or daughterboard • serial advanced technology attachment (SATA) • eSATA • power supply components: • AC adapter • ATX proprietary • pins (20, 24) • voltage selector switch • voltage, wattage and capacity • storage devices and backup media components: • floppy disk drive (FDD) • hard disk drive (HDD): solid state versus magnetic • optical drives, such as CD, DVD, RW or blu-ray • removable storage: • external CD-RW and hard drive • hot swappable devices and non-hot swappable devices • solid state (e.g. thumb drive, flash, SD cards, USB) • Tape drive.

Organizational guidelines may include:	• communication methods • content of emails • dispute resolution • document procedures and templates • downloading information and accessing particular websites • financial control mechanisms • opening mail with attachments • personal use of emails and internet access • Virus risk.
Appropriate person may include:	• authorised business representative • client • Supervisor
Clients may include:	• department within the organisation • person within a department • Third party.
Organizational requirements may include:	• how and what the organisation wants in regard to work environment • preventative maintenance and diagnostic policy • problem solution processes • roles and technical responsibilities in the IT department • Vendor and product service level support agreements.

Evidence Guide	
Critical Aspects of Competence	• Demonstrates a knowledge and skills of: • identify and categorise the different types of internal hardware components • modify system's hardware to meet client requirements • plan the modification and connect internal hardware components according to vendor and technical specifications • Install components across a variety of situations and account for unexpected contingencies.
Required Knowledge and Attitudes	• Demonstrates knowledge of: • areas of the operating system relevant to configuration and testing • current industry-accepted hardware and software products • environmental considerations in e-waste disposal • organizational guidelines and organizational requirements with regard to safety, recycling and component installation • system's diagnostic software and current functionality • Vendor specifications and requirements for component installation.
Required Skills	Demonstrates and communication skills to:

	• consult with peers and supervisors, and internal and external clients • interpret technical computer installation manuals • interpret user manuals and help functions literacy skills to: • organise resources for one-to-one instruction plan, prioritise and organise work write technical reports and maintain records planning and organisational skills to address technical issues problem-solving skills to anticipate and respond to a range of driver-related errors that may arise technical skills to: • Comprehend how the operating system will communicate with the installed component install components test components using available technology test system performance.
Resource Implications	• Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Methods of Assessment	Competence may be assessed through: • Interview / Written Test • Observation / Demonstration with Oral Questioning
Context of Assessment	Competence may be assessed in the work place or in a simulated work place setting.

TOP

Occupational Standard: Hardware and Network Servicing II	
Unit Title	**Apply Problem -Solving Techniques to Routine Malfunction**
Unit Code	**EIS HNS2 07 1221**
Unit Descriptor	This unit defines the competence required to apply problem solving techniques to determine the origin and plan for the resolution of a routine malfunction.

Elements	Performance Criteria
1. Identify problems	1.1 ***Hardware*, *software*, *user*** or procedural ***problem*** areas are identified to ***appropriate person*** in the organization 1.2 Problems to be investigated are defined and determined 1.3 Current conditions of the ***hardware, software, user*** and problems are objectively identified and documented
2. Determine fundamental / root causes of the problem	2.1 Possible causes are identified based on experience and the use of diagnostic tools and analytical techniques. 2.2 Possible cause statements are developed based on findings 2.3 Fundamental causes are identified per results of diagnosis and investigation conducted
3. Recommend solutions to problem	2.1 Potential ***solutions*** to problems are identified 2.2 Recommendations about possible solutions are developed, documented, ranked and presented to the appropriate person for decision 2.3 Implementation and evaluation of solutions are planned 2.4 Recommended solutions are documented and submitted to the appropriate person for confirmation
4. Participate in Workplace Communication	4.1 Effective questioning, active listening and speaking skills are used to gather and convey information. 4.2 Defined workplace procedures for the location and storage of information are used 4.3 Workplace data is recorded on standard workplace forms and documents. 4.4 Basic mathematical processes are used for routine calculations.

Variable	Range
Occupational Health & Safety (OH&S)	May include but not limited to: Correct posture, lighting, type of desk, type of monitor, style of chair, typing position, repetitive strain injury prevention, ventilation, light position, correct lifting method, and length of time in front of computer. May also include licensing-related and physical safety considerations such as general electrical safety and cabling, power supply and leads as they apply to computer and peripheral installations.
Appropriate person	May include but not limited to: • a supervisor, teacher, authorized business representative or client
Hardware	May include but not limited to: • Workstations, personal computers • Modems or other connectivity devices • Networks • Remote sites • Servers
Software	May include but not limited to: • commercial, in-house, packaged or customized software
User	May include but not limited to: • a person within a department, a department within the organization or a third party
Problem	May include but not limited to: • routine malfunctions or problems that affect the immediate work environment, particularly in relation to using equipment such as workstations, keyboards, peripherals
Solutions	May include but not limited to: • new hardware, hardware upgrades, new software, software upgrades, user training or implementing a new system
Tools and equipment	May include but not limited to: • Basic computer maintenance tool kit & Safety tools • Computer • Antivirus software & Recovery software • Password cracker (hiren boot, live boot, wondershare and etc.

Evidence Guide	
Critical Aspects of Competence	Assessment must confirm the ability to • apply problem solving techniques to determine the root cause of a routine malfunction or to refer the problem according to escalation procedures • recommend solution to the problem

Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • Broad knowledge of help desk and maintenance practices • Current industry-accepted hardware and software products, with broad knowledge of general features and capabilities and detailed knowledge in some areas • Broad knowledge of the operating system • Broad knowledge of current industry practices • Broad knowledge of diagnostic tools • Decision making within a limited range of options • Clear and precise communication that varies according to audience • Team participation • Time management as applied to self-management • Analytical skills in relation to routine malfunctions • Customer service skills • Questioning and active listening to clarify general information
Underpinning Skills	Demonstrates skills to: • Identify problems • Using range of formal problem solving techniques • Identifying and clarifying the nature of the problem • Devising and recommending the best solution to the problem • Evaluating the solution
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing II	
Unit Title	**Care for Network and Computer Hardware**
Unit Code	**EIS HNS2 08 1221**
Unit Descriptor	This unit defines the competence required to maintain computer hardware. It includes locating sitting of hardware for safe and efficient utilization and reducing risk of infection.

Elements	Performance Criteria
1. Identify computer hardware components	1.1 ***External hardware*** components and peripherals are identified based on business requirement 1.2 ***Internal hardware*** components are identified as needed 1.3 Requirements specified by ***hardware*** manufacturers are reviewed, recorded and applied where appropriate. 1.4 Quality standards of hardware components and associated ***peripherals*** are determined and recorded 1.5 Relationship of computer hardware and software is determined and established for proper functioning of the system 1.6 ***Safe work*** *practices* are determined, recorded and applied, taking into account legal and manufacturer requirements
2. Establish location requirements for hardware and peripherals	2.1 Suitable environmental conditions are determined and applied for hardware and peripherals 2.2 General orientation and proper functioning of different ***computer platforms*** are considered in locating computer 2.3 ***System protection devices*** are determined and applied to keep hardware form damage. 2.4 Requirements are determined and applied when moving hardware. 2.5 Suitable storage principles are determined and applied for hardware and associated *peripherals* and media. 2.6 ***Business requirements*** are considered and applied in respect of hardware location 2.7 Functions of computer *hardware* and associated ***OHS standards*** and ***environmental concerns*** are considered
3. Monitor threats to the network	3.1 Use third-party software or utilities to evaluate and report on system security 3.2 Review logs and audit reports to identify ***security threats***

	3.3 Carry-out spot checks and other ***security strategies*** to ensure that procedures are being followed 3.4 Investigate and implement inbuilt or additional ***encryption*** facilities 3.5 Prepare and present an audit report and recommendations to appropriate person 3.6 Obtain approval for recommended changes to be made
4. Establish maintenance practices	3.1 Maintenance requirements specified by the ***equipment*** manufacturer are determined. 3.2 ***Maintenance*** schedules including removal of dust and grease build -up are produced 3.3 Diagnostic functions including replacing suspect ***components*** with other serviceable components and reloading of associated software are performed 3.4 Software security settings to prevent destructive software from infecting the computer are configured 3.5 Unserviceable components are determined whether replaceable through warranty, replacement or upgrade 3.6 Diagnostic functions are performed using the ***operating system*** and third-party diagnostic tools

Variable	**Range**
External hardware	May include but not limited to: • screen, keyboard, mouse, disk drives, USB, serial and parallel ports
Internal hardware components	May include but are not limited to: CPU, memory chip, motherboard, video display card, network interface card, sound card, cabling.
Hardware	May include but not limited to workstations, personal computers, modems and other connectivity devices, networks, DSL modems, remote sites, servers
Peripherals	may include but are not limited to: • Printers, scanners, tape cartridges • Speakers, multimedia kits • Personal computer fax/modems
Safe work	May include correct posture, lighting, type of desk, type of monitor, style of chair, typing position, correct lifting method, repetitive strain injury prevention, ventilation, light position and length of time in front of computer
Computer platforms	May include but are not limited to: Apple Macintosh and PCs, and the various operating systems used on each.
System protection devices	May include but are not limited to surge protection and uninterruptible power supplies

Business requirements	May include cost and quality, robustness, industry standard components and capability for further system upgrades
Environmental concerns	May include but is not limited to: • recycling, safe disposal of packaging (e.g. cardboard, polystyrene, paper, plastic) and correct disposal of redundant hardware (e.g. motherboards, hard drives, circuit boards) by an authorized body • handling of hazardous materials
Security threats	May include eavesdropping, manipulation, impersonation, penetration, denial of service, by-pass, hacking, viruses
Security strategies	May include privacy, authentication, authorization and integrity, and usually relates directly to the security objectives of the organization.
Encryption facilities	May include features or protocols such as RSA public key, PGP (pretty good privacy), symmetric ciphers, asymmetric public-key ciphers, sniffers, PKI, SSH, Deslogin, PKZIP, secure socket layer (SSL), digital signatures
Occupational Health and Safety (OHS)	OHS precautions and measures may include against: • Physical hazards – impact, illumination, pressure, noise, vibration, temperature, radiation • Chemical hazards – dusts, fibers, mists, fumes, smoke, gasses, vapors • Ergonomics ▪ Psychological factors – over exertion/ excessive force, awkward/static positions, fatigue, direct pressure, varying metabolic cycles ▪ Physiological factors – monotony, personal relationship, work out cycle • Burglary, Fire and Power accidents such as handling of mains electricity and handling of high-impedance devices
equipment	May include: • mouse, touch pad, keyboard, pens • mobile phones, palmtops and personal digital assistants (PDAs), laptops and desktop computers • bluetooth devices, universal serial bus (USB), firewire (IEEE 1394)
Maintenance	May include on-site response, remote diagnostics or return to depot
Components	May include motherboards, CMOS battery, central processing unit (CPU), CD and DVD drives, interface cards, drives fax/modem cards, RAM upgrades, CPU upgrades.
Operating system	May include but is not limited to Linux 6.0 or above, Windows 7 or above, Apple OS 8 or above

Evidence Guide

Critical aspects of Competence	Assessment must ensure the ability to – • establish safe work practices • establish sitting requirements for system hardware and associated peripheral devices • establish maintenance practices and determine appropriate hardware quality standards • determine, select, explain and use hardware components, peripheral equipment and consumables correctly and efficiently according to the task requirement • identify and monitor threats to network
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • Ergonomic principles to avoid back, wrist and eye strain • Basic knowledge of current industry-accepted hardware and software products, with broad knowledge of general features and capabilities • OHS principles and responsibilities; and specific to equipment powered by mains electricity • Viruses, worms and other security issues • System hardware and associated peripherals functions • Potential environmental effects of common types of hardware • Importance of maintenance • Handling of high-impedance devices • Span of quality levels in common hardware • Systems technologies, with broad knowledge of general features and capabilities and substantial depth in some areas • Risk analysis, with broad knowledge of general features • Broad knowledge of specific security technology • Broad knowledge of privacy issues and legislation
Underpinning Skills	Demonstrates skills to: • Determine best location for hardware and peripherals • Determine hardware quality standards • Identify computer Hardware components • Report writing skills for business requiring depth in some areas, analysis and evaluation of information in a defined range of areas
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing II	
Unit Title	**Update and Document Operational Procedures**
Unit Code	**EIS HNS2 09 1221**
Unit Descriptor	This unit defines the competence required to assess, update and document the operational procedures required to use the system.

Elements	Performance Criteria
1. Assess technical and user documentation	1.1 Current version of ***technical and user documentation*** is reviewed based on the latest operational procedures. 1.2 Accuracy of technical and user documentation is compared with current ***system*** functionality. 1.3 Inaccuracies are identified and documented for future reference.
2. Update procedures	2.1 Operational procedure requirements are determined using review outcomes. 2.2 Operating procedures are developed / updated for the system. 2.3 Proposed operating procedures are submitted to ***appropriate person***.
3. Update documentation	3.1 Feedback is reviewed and appropriate changes are made as needed. 3.2 Technical and user documentation are updated to incorporate changes. 3.3 Technical and user documentation are submitted to appropriate person for final approval. 3.4 Technical and user documentation are distributed as agreed with appropriate person.
4. Work in Team Environment	4.1 ***Role and objective of the team*** is identified from available ***sources of information*** 4.2 Team parameters, reporting relationships and responsibilities are identified from team discussions and appropriate external sources 4.3 Individual role and responsibilities within the team environment is identified 4.4 Roles and responsibility of other team members are identified and recognized 4.5 Reporting relationships within team and external to team are identified

	4.6 Effective and appropriate forms of communications used and interactions undertaken with team members who contribute to known team activities and objectives 4.7 Contribution is made to the development of team work plans based on understanding of team's role and objectives and individual competencies of the members

Variable	**Range**
Occupational Health & Safety (OH&S)	OHS precautions and measures may include against: • Physical hazards – impact, illumination, pressure, noise, vibration, temperature, radiation • Chemical hazards – dusts, fibers, mists, fumes, smoke, gasses, vapors • Ergonomics ▪ Psychological factors – over exertion/ excessive force, awkward/static positions, fatigue, direct pressure, varying metabolic cycles ▪ Physiological factors – monotony, personal relationship, work out cycle ▪ Burglary ▪ Fire ▪ Power accidents
Tools and Equipment	• Documentation and manuals • Soft wares
Types and Sources of Information	• Internet • System or project related documentation • Staffing resources • Technical and user documentation • Operational procedure
Technical and user documentation	May include system or project specifications, system design, system functionality, reports, help references, technical manuals, operational procedures, training materials and self-paced tutorials, help and Support Function, user guides and brochures.
System	May include but is not limited to networks, software, databases, applications, servers, operating systems, gateways.
Appropriate person	May include a supervisor, teacher, authorized business representative or client

Evidence Guide	
Critical aspects of Competence	Assessment must confirm the ability to manage the production of clear, easy-to-read procedures conforming to required standards for the utilization of the specified system.

Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • documentation standards and tools • client business domain • role of stakeholders and the degree of stakeholder involvement • current industry-accepted hardware and software products • current business practices in relation to preparing reports
Underpinning Skills	Demonstrates skills to: • review and update technical and user documentation • update procedures • update documentation
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network servicing II	
Unit Title	**Record Client Support Requirements**
Unit Code	**EIS HNS2 10 1221**
Unit Descriptor	This unit defines the competence required to record, prioritize and escalate client support requests.

Elements	Performance Criteria
1. Log requests for support	1.1 ***Client*** support requests and requirements are recorded according to ***organizational standards*** 1.2 Client support history and details are reviewed 1.3 The information is checked and requested for accuracy and urgency according to organizational standards
2. Prioritize support requests with appropriate personnel	2.1 Relevant guidelines are identified for prioritizing or rating client requests 2.2 Client requests are prioritized based on its criticality or impact on the business 2.3 Requests are referred to an ***appropriate person*** or department for assistance 2.4 Appropriate persons involved with client support are to be communicated
3. Receive and Respond to Workplace Communication	3.1 Required information is gathered by listening attentively and correctly interpreting or understanding information/ instructions. 3.2 Instructions/information are properly recorded. 3.3 Instructions are acted upon immediately in accordance with information received 3.4 Written notices and instructions are read and interpreted correctly in accordance with organizational guidelines 3.5 Routine written instruction is followed in sequence 3.6 Feedback is given to workplace supervisor based on the instructions/information received

Variable	Range
Client	May include but not limited to: • internal departments, external organizations, individual people and employees
Organizational standards	May include but not limited to: • Variables may include but are not limited to: • Security procedures • Logged call procedures • Client liaison policy • Escalation procedures • Preventative maintenance and diagnostic policy • Roles and technical responsibilities in the IT department • Vendor and product service-level support agreements
Appropriate person	May include but not limited to: • a supervisor, teacher, vendor business representative, help desk person or subject matter expert
Evidence Guide	
Critical aspects of Competence	Assessment must confirm the ability to: • accurately log calls and record, • prioritize and escalate client support requests according to organizational policy and procedures
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • organizational procedures for rating and prioritizing client requests • broad knowledge of escalation procedures • roles and responsibilities of it division • broad knowledge of maintenance procedures • business scheduling requirements • current business practices in relation to preparing reports and documents • broad knowledge of diagnostic tools

	• basic analytical concepts for questioning and gathering information
Underpinning Skills	Demonstrates skills to: • log requests for support • perform questioning and active listening in clarifying client requirements and gathering important information • customer service skills in relation to receiving requests for support • skills in handling difficult clients in relation to receiving requests for support • conflict resolution skills in relation to receiving requests for support • writing reports and workplace documentation
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level II	
Unit Title	**Prevent and Eliminate MUDA**
Unit Code	**EIS HNS2 11 1221**
Unit Descriptor	This unit covers the knowledge, skills and attitude required by a worker to prevent and eliminate MUDA/wastes in his/her workplace by applying scientific problem-solving techniques and tools to enhance quality, productivity and other kaizen elements on continual basis It covers responsibility for the day-to-day operation of the work and ensures Kaizen Elements are continuously improved and institutionalized.

Element	Performance Criteria
1. Prepare for work.	1.1. Work instructions are used to determine job requirements, including method, material and equipment. 1.2. Job specifications are read and interpreted following working manual. 1.3. ***OHS requirements***, including dust and fume collection, breathing apparatus and eye and ear personal protection needs are observed throughout the work. 1.4. Appropriate material is selected for work. 1.5. ***Safety equipment and tools*** are identified and checked for safe and effective operation.
2. Identify MUDA and problem	2.1 Plan of MUDA and problem identification is prepared and implemented. 2.2 Causes and effects of MUDA are discussed. 2.3 All possible problems related to the process /Kaizen elements are listed using ***statistical tools and techniques***. 2.4 All possible problems related to kaizen elements are identified and listed on Visual Management Board/Kaizen Board. 2.5 ***Tools and techniques*** are used to draw and analyze current situation of the work place. 2.6 Wastes/MUDA are identified and measured based on ***relevant procedures***. 2.7 Identified and measured wastes are reported to relevant personnel.
3. Analyze causes of a problem.	3.1 All possible causes of a problem are listed. 3.2 Cause relationships are analyzed using***4M1E***. 3.3 Causes of the problems are identified. 3.4 The root cause which is most directly related to the problem is selected.

	3.5 All possible ways are listed using ***creative idea generation*** to eliminate the most critical root cause. 3.6 The suggested solutions are carefully tested and evaluated for potential complications. 3.7 Detailed summaries of the action plan are prepared to implement the suggested solution.
4. Eliminate MUDA and Assess effectiveness of the solution.	4.1. Plan of MUDA elimination is prepared and implemented by ***medium KPT*** members. 4.2. Necessary attitude and the ***ten basic principles*** for improvement are adopted to eliminate waste/MUDA. 4.3. Tools and techniques are used to eliminate wastes/MUDA based on the procedures and OHS. 4.4. Wastes/MUDA are reduced and eliminated in accordance with OHS and organizational requirements. 4.5. ***Tangible and intangible results*** are identified. 4.6. Tangible results are compared with targets using ***various types of diagrams***. 4.7. Improvements gained by elimination of waste/MUDA are reported to relevant bodies.
5. Prevent occurrence of wastes and sustain operation.	5.1. Plan of MUDA prevention is prepared and implemented. 5.2. Standards required for machines, operations, defining normal and abnormal conditions, clerical procedures and procurement are discussed and prepared. 5.3. Occurrences of wastes/MUDA are prevented by using ***visual and auditory control methods***. 5.4. Waste-free workplace is created using ***5W and 1H***sheet. 5.5. The completion of required operation is done in accordance with standard procedures and practices. 5.6. The updating of standard procedures and practices is facilitated. 5.7. The capability of the work team that aligns with the requirements of the procedure is ensured and trained on the new ***Standard Operating Procedures (SOPs)***.

Variable	**Range**
OHS requirements	May include, but not limited to: • Are to be in accordance with legislation/ regulations/codes of practice and enterprise safety policies and procedures. This may include protective clothing and equipment, use of tooling and equipment, workplace environment and safety, handling of material, use of fire fighting equipment, enterprise first aid, hazard control and hazardous materials and substances. • PPE are to include that prescribed under legislation/regulations/codes of practice and workplace policies

	and practices. • Safe operating procedures are to include, but are not limited to the conduct of operational risk assessment and treatments associated with workplace organization. • Emergency procedures related to this unit are to include but may not be limited to emergency shutdown and stopping of equipment, extinguishing fires, enterprise first aid requirements and site evacuation.
Safety equipment and tools	May include, but not limited to: • Dust masks/goggles • Glove • Working cloth • First aid and • Safety shoes
Statistical tools and techniques	May include, but not limited to: • 7 QC tools May include, but not limited to: ➢ Stratification ➢ Pareto Diagram ➢ Cause and Effect Diagram ➢ Check Sheet ➢ Control Chart/Graph ➢ Histogram and Scatter Diagram • QC techniques May include, but not limited to: ➢ Brain storming ➢ Why analysis ➢ What if analysis ➢ 5W1H
Tools and techniques	May include, but not limited to: • Plant Layout • Process flow • Other Analysis tools • Do time study by work element • Measure Travel distance • Take a photo of workplace • Measure Total steps • Make list of items/products, who produces them and who uses them & those in warehouses, storages etc. • Focal points to Check and find out existing problems • 5S • Layout improvement • Brainstorming

	• Andon • U-line • In-lining • Unification • Multi-process handling &multi-skilled operators • A.B. control (Two-point control) • Cell production line • TPM (Total Productive Maintenance)
Relevant procedures	May include, but not limited to: • Make waste visible • Be conscious of the waste • Be accountable for the waste and measure the waste.
4M1E	May include, but not limited to: • Man • Machine • Method Material and Environment
Creative idea generation	May include, but not limited to: • Brainstorming • Exploring and examining ideas in varied ways • Elaborating and extrapolating • Conceptualizing
Medium KPT	May include, but not limited to: • 5S • 4M (Machine, Method, Material and Man) • 4p (Policy, Procedures, People and Plant) • PDCA cycle Basics of IE tools and techniques
The ten basic principles for improvement	May include, but not limited to: • Throw out all of your fixed ideas about how to do things. • Think of how the new method will work- not how it won. • Don’t accept excuses. Totally deny the status quo. • Don’t seek perfection. A 5o percent implementation rate is fine as long as it’s done on the spot. • Correct mistakes the moment they are found. • Don’t spend a lot of money on improvements. • Problems give you a chance to use your brain. • Ask “why?” At least five times until you find the ultimate cause. • Ten people’s ideas are better than one person. • Improvement knows no limits.

Tangible and intangible results	May include, but not limited to: • Tangible result may include quantifiable data • Intangible result may include qualitative data
various types of diagrams.	May include, but not limited to: • Line graph • Bar graph • Pie-chart • Scatter diagrams • Affinity diagrams
Visual and auditory control methods	May include, but not limited to: • Red Tagging • Sign boards • Outlining • Add ones • Kanban, etc.
5W and 1H	May include, but not limited to: • Who • What • Where • When • Why and • How
Standard Operating Procedures (SOPs).	May include, but not limited to: • The customer demands • The most efficient work routine (steps) • The cycle times required to complete work elements • All process quality checks required to minimize defects/errors • The exact amount of work in process required

Evidence Guide	
Critical Aspects of Competence	Demonstrate knowledge and skills to: • Discuss why wastes occur in the workplace • Discuss causes and effects of wastes/MUDA in the workplace • Analyze the current situation of the workplace by using appropriate tools and techniques • Identify, measure, eliminate and prevent occurrence of wastes by using appropriate tools and techniques • Use 5W and 1H sheet to prevent • Detect non-conforming products/services in the work area • Apply effective problem-solving approaches/strategies. • Implement and monitor improved practices and procedures

	• Apply statistical quality control tools and techniques.
Underpinning Knowledge and Attitude	Demonstrate knowledge of: • Targets of customers and manufacturer/service provider • Traditional and kaizen thinking of price setting • Kaizen thinking in relation to targets of manufacturer/service provider and customer • value • The three categories of operations • the 3“MU” • wastes occur in the workplace • The 7 types of MUDA • QC story/PDCA cycle/ • QC story/ Problem solving steps • QCC techniques • 7 QC tools • The Benefits of identifying and eliminating waste • Causes and effects of 7 MUDA • Procedures to identify MUDA • Necessary attitude and the ten basic principles for improvement • Procedures to eliminate MUDA • Prevention of wastes • Methods of waste prevention • Definition and purpose of standardization • Standards required for machines, operations, defining normal and abnormal conditions, clerical procedures and procurement • Methods of visual and auditory control • TPM concept and its pillars. • Relevant OHS and environment requirements • Method and Lines of communication • Methods of making/recommending improvements. • Reporting procedures • Workplace procedures associated with the candidate's regular technical duties • organizational structure of the enterprise
Underpinning Skills	Demonstrate skills to: • Draw & analyze current situation of the work place • Use measurement apparatus (stop watch, tape, etc.) • Calculate volume and area • Apply statistical analysis tools • Use and follow checklists to identify, measure and eliminate

	wastes/MUDA • Identify and measure wastes/MUDA in accordance with OHS and procedures • Use tools and techniques to eliminate wastes/MUDA in accordance with OHS procedure. • Apply 5W and 1H sheet • Update and use standard procedures for completion of required operation • Apply Visual Management Board/Kaizen Board. • Detect non-conforming products or services in the work area • Work with others • Read and interpret documents • Observe situations • Solve problems • Communicate information • Gather evidence by using different means • Report activities and results using report formats • Implement and monitor improved practices and procedures
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Methods of Assessment	Competence may be assessed through: • Interview/Written Test • Observation/Demonstration with Oral Questioning
Context of Assessment	Competence may be assessed in the work place or in a simulated work place setting.

NQTF Level I

TOP

Occupational Standard: Hardware and Network Servicing Level I	
Unit Title	**Connect Hardware Peripherals**
Unit Code	**EIS HNS1 01 1221**
Unit Descriptor	This unit defines the competence required to connect hardware peripherals according to instructions and a workstation or networked computer to the internet.

Elements	Performance Criteria
1. Confirm requirements of client	1.1 ***Client peripherals*** are identified requirements and confirmed in accordance with ***organizational standards*** 1.2 Client requirements and peripherals needed are documented in line with organizational standards and findings are reported to the appropriate person 1.3 Client requirements are verified with appropriate person in line with organizational standards and reporting procedures 1.4 Action must be taken to ensure client support expectations are covered by vendor warranty and support services
2. Obtain required peripherals	2.1 Peripherals are obtained under instruction from ***appropriate person*** 2.2 Peripherals are entered into equipment inventory according to organizational standards 2.3 Validate those contents of delivered components and physical contents match the packing list and resolve discrepancies, if necessary 2.4 Peripherals are stored according to vendor/manual guidelines
3. Connect hardware peripherals	3.1 Timeframe for installation schedule is verified with the client in accordance with the organization requirements 3.2 Old peripherals are removed and/or replaced with minimum disruption to clients taking into account environmental considerations and ***OHS standards*** 3.3 New peripherals are connected with minimum disruption to clients and taking into account the operating system procedures 3.4 The computer is configured to accept the new peripherals

	3.5 Hardware peripherals are tested and confirm client satisfaction, particular attention must be paid to possible impact on other systems and adjustments are made as required
4. Connect workstation to the internet	4.1 ***Workstations*** are connected to the internet through the existing internet connection and functionality confirmed 4.2 ***Internet browser software*** is launched to enable access to the internet and functionality confirmed

Variable	**Range**
Occupational Health & Safety (OH&S)	May include but not limited to: Occupational health and Safety aspects of relevant organizational activities must be considered May include correct posture, lighting, type of desk, type of monitor, style of chair, typing position, repetitive strain injury prevention, ventilation, light position, correct lifting method, and length of time in front of computer. May also include licensing-related and physical safety considerations such as general electrical safety and cabling, power supply and leads as they apply to computer and peripheral installations
Peripherals	May include but not limited to: • Input equipment may include mouse, touch pad, keyboard, pens, scanners, Web camera, Barcode reader, Finger print scanner. • Output equipment may include printers, Monitor, tape cartridges, speakers • Multimedia kits • Personal computer, modems, Hub/switch, Head/Earphone, photo copier, fax machine • Digital camera, mobile phones, palmtops and personal digital assistants (PDAs), laptops, and desktop computers • Bluetooth devices, universal serial bus (USB), firewire (IEEE 1394), HDMI, SD card Reader
Organizational standards	• Personal use of emails(i.e. Gmail, Hotmail and etc..) and internet access, content of emails, downloading information and accessing particular websites, opening mail with attachments, virus risk (MS windows OS and Mac OS only), dispute resolution, document procedures and templates, communication methods and financial control mechanisms
Appropriate person	supervisor, teacher, authorized business representative or client
Operating system	May include but not limited to:

	• Wins 7,8,10, 11, Sun Solaris/SunOS, HP-UX, AIX, Silicon Graphics IRIX, DEC, VMS, Mac OS X, Linux, NetWare
Client	May include but not limited to: • internal departments, external organizations, individual people and employees
Equipment	May include but not limited to: • workstations, personal computers, modems or other connectivity devices, printers, hard drives, monitors, switches, hubs, personal digital assistant (PDA) and other peripheral devices
OHS standards	May include but not limited to: • correct posture, lighting, Appropriate desk
Internet connection	May include but not limited to: • Ad-hoc, cable, ISDN, broadband or satellite
Business requirements	May include but not limited to: • speed of access, money available, technical support required and other specific internet needs
Features	May include but not limited to: • May be in relation to cost, connectivity, services, connection type and support
Workstation	May include but not limited to: • Personal computers, networked computers, laptops and etc...
Software	May include but not limited to: • commercial, in-house, packaged or customized software
Connection device	May include but not limited to: • ADSL modem, cable modem or ISDN
Vendor instructions	User manual, written instructions from meetings, verbal request or help desk, and search engine references.
Operating system	May include but not limited to: • Linux 7.0 or above, Windows 7 or above, Apple OS X or above
Internet browser software	May include but not limited to: • Netscape Navigator, Internet Explorer, Mozilla, chrome, Opera and others.
Internet	An interconnected system of networks that connects computers around the world via TCP/IP or FTP protocols
Tools and equipment	May include but not limited to: • Organization’s hardware blueprint • Vendor support staff (on call if assessment is a live activity) • Additional staff if required to support the assessment • Hardware peripherals and workstation

	• Personal computer • Internet connection • Modem or other connectivity device • Network tool kits • Paper

Evidence Guide	
Critical aspects of competence	Demonstrates skills and knowledge in: • safely connect hardware peripherals according to vendor instructions with a minimum of down time to the system (competence is required in the connection of five different peripherals) • ability to interpret vendor manuals in relation to the storage and connection of hardware peripherals • application of OHS regulations relating to working with electrical equipment • ability to connect a workstation or networked computers to the internet
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • OHS procedures for electrical equipment • inventory procedures • organizational guidelines relating to external suppliers and vendors • technical systems • operating systems • creating communication with ISP and telecom service organizations • help desk and maintenance practices • current industry-accepted hardware and software products, with broad knowledge of general features and capabilities and detailed knowledge in some areas • input/output devices the range of internet service providers (ISPs) and the varying plans, technologies and services they offer
Underpinning Skills	Demonstrates skills to: • Connect hardware peripherals • Connect workstation to the internet
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace and OHS practices.
Methods of Assessment	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration

Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level I	
Unit Title	**Operate Personal Computer**
Unit Code	**EIS HNS1 02 1221**
Unit Descriptor	This unit defines the competence required to operate a personal computer, including starting the PC, logging in, using and understanding desktop icons and their links to underlying programs, navigating a directory structure, saving work, printing, closing down the PC and word processing.

Elements	Performance Criteria
1. Start and Shutdown the computer	1.1 ***Peripheral device*** connections for correct position are checked 1.2 Input voltage for the device based on the ***OHS standards*** are checked 1.3 Power at both the power button and ***computer*** are switched on 1.4 Save important documents and programs to minimize risk of data loss 1.5 Save any work to be retained and close open application programs 1.6 Shut down computer and switch off any unused peripheral Devices
2. Access basic system information	2.1 User name and password are inserted as prompted and noted access, privacy, security and related conditions of use displayed on introductory screens 2.2 ***Operating system*** are navigated to access ***system information*** to identify system configuration and application versions in operation 2.3 ***help and support functions*** are used as required
3. Navigate and Manipulate desktop environment	3.1 Desktop icons are created and customized 3.2 Desktop icons are selected, opened and closed to access ***application programs*** 3.3 Application windows are manipulated and desktop returned to original conditions
4. Organize basic directory/ folder structure and files	4.1 Directories and subdirectories are created and named 4.2 ***Attributes*** of directories are identified 4.3 Subdirectories between directories are copy and moved 4.4 Directories as required are renamed, Hide/show

	4.5 Directories and subdirectories are accessed via different paths
5. Organize files for user and/or organization requirements	5.1 ***System browser*** are used to search drives for specific files 5.2 Most commonly used types of files in the directories are accessed 5.3 Groups of files are selected, opened and renamed as required 5.4 Files between directories are moved 5.5 Files to ***disks*** are copied/backup 5.6 Deleted files are restored as necessary 5.7 Disks are erased and formatted as necessary
6. Print information	6.1 Printers are added if required and ensured to have correct ***printer settings*** 6.2 Default printer are changed if appropriate 6.3 Information is printed from an installed printer
7. Operate application software	7.1 Documents and customize basic settings are created to meet page layout conventions 7.2 Document and create tables are formatted 7.3 Images and use mail merge are added 7.4 Basic print settings and print documents are selected

Variable	**Range**
Peripheral device	May include but not limited to: • mouse, keyboard, visual display unit, monitor and printer
OHS standards	May include but not limited to: • correct posture, lighting, type of desk, type of monitor, style of chair, typing position, repetitive strain injury prevention, ventilation, light position, correct lifting method, and length of time in front of computer • may also include physical safety considerations such as general electrical safety and cabling, power supply and leads as they apply to computer and peripheral installations
Computer	May include but not limited to: • laptops, workstations, servers or other devices
Operating System	May include but not limited to: • Linux 7.0 or above, Windows 7 or above, Apple OS X or above

System information	May include but not limited to: • hardware and software components that run a computer
Help and support functions	• Instruction manual or a portion of the manual, integrated into the program.
Application programs	May include but not limited to: • database programs, word processors, PowerPoint, Publisher, email programs, internet browsers, system browsers and spreadsheets
Attributes	May include but not limited to: • Indicates several properties of the directory, for example, they indicate whether the directory is read-only, whether it needs to be backed up, and whether it is visible or hidden
System browser	May include but is not limited to Windows Internet explorer
Disks	May include but not limited to: • CDs, CD-RW (compact disks-read write), DVD RW, zip disks, flash drives, solid state hard drives
Printer settings	May include but not limited to: • layout, paper size, paper tray, cartridge type, number of copies, orientation

Evidence Guide	
Critical aspects of competence	• Must confirm the ability to use software, navigate around the desktop, use system features to perform tasks, and save results of work • Must ensure the ability to create open and retrieve documents, customize basic settings, format documents, create tables, add objects and images, and save and print documents
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • Organizational benchmarks for minimum typing skills, including speed and accuracy • Creating and opening documents • Formatting documents • Inserting tables and images • Saving, printing and closing documents • Mail merge function • Basic keyboarding skills • Computer functions • Basic parts of a computer and various hardware components • Storage devices and basic categories • Basic software operation
Underpinning Skills	Demonstrates skills to: • Access basic system information • Operate application software
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace and OHS practices.

Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level I	
Unit Title	**Protect Application or System Software**
Unit Code	**EIS HNS1 03 1221**
Unit Descriptor	This unit defines the competence required to keep application or system software working effectively. It includes detecting and removing destructive software

Elements	Performance Criteria
1. Ensure user accounts are controlled	1.1 Check whether you logon by Administrator or not. 1.2 Modify default user settings to ensure that they conform to security policy 1.3 Previously created user settings are modified to ensure they conform to updated security policy 1.4 Ensure legal notices displayed at logon are appropriate 1.5 Appropriate utilities are used to check strength of passwords and consider tightening rules for password complexity 1.6 Emails are monitored to uncover breaches in compliance with legislation 1.7 information services are accessed to identify security gaps and take appropriate action using hardware and software or patches
2. Detect and remove destructive software	2.1 Common types of ***destructive software*** are defined and identified 2.2 ***Virus protection*** compatible with the ***operating system*** in use are selected and installed 2.3 Advanced systems of protection are described in order to understand allow/disable and further options 2.4 ***Software updates*** on a regular basis are installed 2.5 Software security settings are configured to prevent destructive software from infecting computer 2.6 Virus protection software are run and/or scheduled on a regular basis 2.7 Detected destructive software are reported to appropriate person and remove the destructive software
3. Identify and take action to stop spam	3.1 Common types of ***spam*** are defined and identified 3.2 ***Appropriate action*** is taken in order to protect unauthorized access of spammers

	3.3 Spam filters are configured and used 3.4 Spams are reported and documented to identify the security threats and be able to perform recommended action

Variable	Range
Destructive Software	May include but not limited to: • Viruses, File viruses, System sector viruses, Macro viruses, Worms, Trojans, Logic bombs and Spy ware
Virus protection	May include but not limited to: • There are various antivirus software applications available. Some include: F-Secure, McAfee, Panda Antivirus, Protector Plus Antivirus, Symantec's Norton Antivirus, Command Antivirus, Vet. AMI virus, Smadav, Avast and etc...
Operating system	May include but not limited to: • Linux 6.0, 7.0 or above, Windows 7 or above, Apple OS 8 or above
Software Updates	May include but not limited to: • Service packs and service releases, Security patches, Automatic online updates, and Virus scanning engine Updates and Virus definition updates
Spam	May include but not limited to: • unsolicited commercial electronic messaging, where electronic messaging covers emails, instant messaging, SMS and other mobile phone messaging, but does not cover normal voice-to-voice communication by telephone
Appropriate action	May include but not limited to: • Delete the spam • Block the sender by configuring spam filter. • Unsubscribe from mailing list, if company is reputable.
Maintenance	May include but not limited to: • on-site response, remote diagnostics or return to depot
Tools and equipment	May include but not limited to: • appropriate software and diagnostic tools • computer hardware • records and reports

Evidence Guide	
Critical aspects of Competence	Assessment must ensure the ability to establish : • safe work practices, • Siting requirements for system hardware and associated peripheral devices. • maintenance practices and determine appropriate hardware quality standards • Assessment must confirm the ability to identify, isolate and protect a system from destructive software by installing virus protection and software updates and to identify and take counter-action against SPAM.
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • General OH&S principles and responsibilities • OH&S principles specific to equipment powered by mains electricity • Viruses, worms and other security issues • System hardware and associated peripherals functions • Potential environmental effects of common types of hardware • Importance of maintenance • Handling of high-impedance devices • Communication skills • Span of quality levels in common hardware • Software related to hardware operations • Basic knowledge of identification of spam and virus intrusions and appropriate remedial action • Broad general knowledge of operating systems supported by the organization • Broad general knowledge of computer hardware • Basic knowledge types protective applications used against viruses and spam • Spam Act and associated guidelines
Underpinning Skills	Demonstrates skills to: • Establish location requirements for hardware and peripherals • Establish maintenance practices
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration

Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level I	
Unit Title	**Install Software Application**
Unit Code	**EIS HNS1 04 1221**
Unit Descriptor	This unit defines the competence required to install or upgrade basic software applications using a commercial applications program.

Elements	Performance Criteria
1. Determine software and upgrade requirements	1.1 ***Client*** requirements are documented and reported to appropriate person in accordance with the workplace standard 1.2 Act on instructions to meet client requirements in line with organizational requirements
2. Obtain software or software upgrade	2.1 ***Application program*** that best conforms to requirements and organizational policies are investigated and selected 2.2 Application program under instruction is obtained from appropriate person 2.3 ***Licensing requirements*** and record are determined in line with organizational guidelines 2.4 Target ***computer*** is ensured to conform with the minimum ***hardware*** and ***operating system*** requirements of the application program
3. Install or upgrade software	3.1 New or **upgraded *software*** are installed in accordance with appropriate person or organizational instructions 3.2 Installation process is completed efficiently and effectively with minimal disruption 3.3 Testing and acceptance are carried out in line with corporate guidelines, paying particular attention to possible ***impact*** on other systems 3.4 Ensure client requirements are satisfied in accordance with the ***organizational standard*** 3.5 Outstanding client issues are referred to appropriate person as necessary

Variable	Range
Client	May include but not limited to: • internal departments, external organizations, individual people and internal employees
Application program	May include but not limited to: • database programs, MS-Office, email programs, internet browsers ,system browsers, Anti-virus and spreadsheets
Licensing requirements	May include but not limited to: • type of license, cost of license, support provided, and number of licenses required
Computer	May include but not limited to: • laptops, workstations and servers
Hardware	May include but not limited to: • workstations, personal computers • modem or other connectivity device, including DSL modems • networks • remote sites • servers
Operating System	May include but not limited to: • Linux 7.0 or above, Windows 7 or above, Apple OS X or above.
Upgraded *software*	May include but not limited to: • Commercial software applications(MS-office 2007 and above); organization-specific software
Impact	May be in relation to installation time, effect on normal business, problems and data entry.
Organizational requirements	May include but not limited to: • guidelines, corporate purchasing, licensing arrangements and budget
Occupational Health and Safety (OHS)	May include but not limited to: • correct posture, lighting, and type of desk, type of monitor, style of chair, typing position, repetitive strain injury prevention, ventilation, light position, correct lifting method, and length of time in front of computer • licensing-related and physical safety considerations such as general electrical safety and cabling, power supply and leads as they apply to computer and peripheral installations
Tools and equipment	May include but not limited to: • basic computer maintenance tool kit • computer, antivirus software , recovery software, safety tools

Evidence Guide	
Critical aspects of Competence	• Assessment must confirm the ability to install software applications through operating system instructions • Configure computer to accept new software or upgrade.
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • organizational guidelines for purchasing • licensing arrangements and responsibilities • software copyright responsibilities • operating systems supported by the organization • hardware storage devices • input/output devices • client business domain • technical writing and reporting
Underpinning Skills	Demonstrates skills to: • determine software or software upgrade requirements • provide general customer service • perform decision making in a limited range of options • problem solving of known problems in routine procedures • plain English literacy and communication skills in relation to the presentation of information • report writing skills for business requiring some analysis and evaluation of information in a defined range of areas
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level I	
Unit Title	**Develop Keyboard Skills**
Unit Code	**EIS HNS1 05 1221**
Unit Descriptor	This unit describes the performance outcomes, skills and knowledge required to develop basic keyboard skills using touch typing techniques.

Elements	Performance Criteria
1. Use safe work practices	1.1 Workspace, furniture and equipment are adjusted to suit user ***ergonomic requirements***
	1.2 ***Work organization*** is ensured to meet organizational and Occupational Health and Safety (OHS) requirements for computer operation
	1.3 Established ***safety procedures*** are followed when conducting work
2. Identify and develop keyboard skills	2.1 Keyboard functions are identified and applied for both alpha and numeric keyboard functions
	2.2 ***Touch typing technique*** is applied to complete a task
	2.3 ***Speed and accuracy*** are developed in accordance with workplace requirements for level of responsibility
3. Check accuracy	3.1 Document is proofread carefully to identify errors
	3.2 Document and correct errors are amended
	3.3 A final document accuracy check is completed

Variable	Range
Ergonomic requirements	may include but not limited to: • avoiding radiation from computer screens • chair height, seat and back adjustment • document holder • footrest • keyboard and mouse position • lighting • noise minimisation • posture • screen position • workstation height and layout

Safety procedures	may include but not limited to:: • completing required documentation • local, state and federal legislation • Materials Safety Data Sheets (MSDSs) • National Health and Medical Research Council guidelines • following OHS guidelines relevant to workplace • maintenance and use of cleaning apparatus in a work environment, such as: ➢ disposing of spilled substances, dangerous products, 'sharps' and waste correctly ➢ maintaining stocks of cleaning equipment (e.g. disposable gloves, liquid repellent aprons, disinfectant) ➢ sterilizing and/or disposing of cleaning equipment ➢ using appropriate cleaning equipment to clean spillages and breakages ➢ wearing protective clothing, protective eye wear when in contact with body fluids or chemicals that may splash • using and storing toxic and hazardous materials correctly • keeping workplace clean and tidy • office practice manual • displaying health and safety brochures, magazines and other material • undergoing operator training when using new equipment or processes special guidelines in a medical setting
Work organization	may include but not limited to: • exercise breaks • mix of repetitive and other activities • rest periods • visual display unit (VDU) eye testing
Touch typing technique	may vary according to: • level of competency of operator • workplace requirements
Speed and accuracy	must be: • consistent with degree of experience of operator • relevant to level of responsibility

Evidence Guide	
Critical aspects of Competence	Evidence of the following is essential: • applying touch typing technique to enter alphanumeric characters • safely using keyboard

Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • key provisions of relevant legislation from all forms of government that may affect aspects of business operations, such as OHS • Organizational benchmarks for keyboarding.
Underpinning Skills	Demonstrates skills to: • communication skills to identify lines of communication, to request advice, to effectively question, to follow instructions and to receive feedback • literacy skills to identify work requirements, to comprehend basic workplace documents, and to produce and proofread simple documents • problem-solving skills to solve routine problems in the workplace, while under direct supervision • technology skills to use equipment safely while under direction, and to use basic keyboard, touch typing and mouse skills to produce simple documents
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competence may be assessed through: • Interview / Written Test • Observation / Demonstration
Context of Assessment	Competence may be assessed in the work place or in a simulated work place setting.

TOP

Occupational Standard: Hardware and Network Servicing Level I	
Unit Title	**Create and Use Spreadsheets**
Unit Code	**EIS HNS1 06 1221**
Unit Descriptor	This unit describes the performance outcomes, skills and knowledge required to operate spreadsheet applications and perform basic operations, including creating and formatting spreadsheet data, incorporating charts and objects, and customising and printing spreadsheets.

Elements	Performance Criteria
1. Select and prepare resources	1.1 Workspace, furniture and equipment are adjusted to suit user ***ergonomic***, ***work organization*** and Occupational Health and Safety (OHS) ***requirements***
	1.2 Energy and resource ***conservation techniques*** are used to minimise wastage in accordance with organizational and statutory requirements
	1.3 ***Spreadsheet task requirements*** are identified and clarified with relevant personnel as required
2. Create spreadsheets	2.1 Ensure ***data*** is entered, ***checked*** and amended in accordance with organizational and task requirements, to maintain consistency of design and layout
	2.2 Spreadsheet is ***formatted*** using ***software functions***, to adjust page and cell layout to meet information requirements, in accordance with organizational style and presentation requirements
	2.3 Ensure ***formulae*** are used and tested to confirm output meets task requirements, in consultation with appropriate personnel as required
	2.4 Manuals, user documentation and online help are used to overcome problems with spreadsheet design and production
3. Produce simple charts	3.1 ***Chart type*** and design that enables valid representation of numerical data are selected and organizational and task requirements are met
	3.2 Chart is created using appropriate data range in the spreadsheet
	3.3 Chart type and layout are modified using formatting ***features***
4. Finalise spreadsheets	4.1 Spreadsheet and any accompanying charts are previewed, adjusted and ***printed*** in accordance with organizational and task requirements

	4.2 Ensure data input meets ***designated time lines*** and organizational requirements for speed and accuracy 4.3 Spreadsheet is named and ***stored*** in accordance with organizational requirements and exit the application without data loss/damage

Variable	Range
Ergonomic requirements	May include but not limited to: • avoiding radiation from computer screens • chair height, seat and back adjustment • document holder • footrest • keyboard and mouse position • lighting • noise minimisation • posture • screen position • workstation height and layout
Work organization requirements	may include but not limited to: • exercise breaks • mix of repetitive and other activities • rest periods
Conservation techniques	may include but not limited to: • double-sided paper use • recycling used and shredded paper • re-using paper for rough drafts (observing confidentiality requirements) • utilising power-save options for equipment
Spreadsheet task requirements	may include but not limited to: • data entry • output • presentation • storage
Data	may include but not limited to: • numbers • text
Checking	may include but not limited to: • accuracy of data • accuracy of formulae with calculator • ensuring instructions with regard to content and format have been followed • proofreading • spelling, electronically and manually
Formatting	may include but not limited to: • alignment on page

	• efficiency of formulae • enhancements to format - borders, patterns and colours • enhancements to text • headers/footers • use of absolute and relative cell addresses • use of cell addresses in formulae
Software functions	may include but not limited to: • adding/deleting columns/rows • formatting cells • formatting text • headers/footers • sizing columns/rows
Formulae	may include but not limited to: • absolute cell referencing and/or mixed references • average • division • maximum • minimum • multiplication • subtraction • sum • combinations of above
Chart types	may include but not limited to: • area • bar • column • exploded pie • line • pie and 3-D pie • scatter/bubble • stacked/multiple bar • stacked, 3-D column
Features	may include but not limited to: • axes • axis title • borders • chart title • colours • data labels • data tables • fills • gridlines • legend • lines • patterns
Printing	may include but not limited to:

	• fit on one page • fit specific number of pages • with formulae • with values
Designated time lines	may include but not limited to: • organizational time line e.g. financial requirements • time line agreed with internal/external client • time line agreed with supervisor/person requiring spreadsheet
Storing data	may include but not limited to: • authorised access • filing locations • organizational policy for backing up files • organizational policy for filing hard copies of spreadsheets • security • storage in electronic folders/sub-folders • storage on CD-ROM, zip drives, USB memory

Evidence Guide	
Critical aspects of Competence	Evidence of the following is essential: • designing a minimum of two spreadsheets • using cell-based formulae • creating charts using relevant data • knowledge of purpose and range of use of spreadsheet functions
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • formatting of workplace documents • organizational requirements for ergonomic standards, work periods and breaks, and conservation techniques • organizational guidelines on spreadsheet manipulation and processing • purpose and range of use of spreadsheet functions
Underpinning Skills	Demonstrates skills to: • communication skills to clarify requirements of spreadsheet • editing and proofreading skills to check own work for accuracy • keyboarding skills to enter text and numerical data • literacy skills to read and understand organization's procedures, and to use basic models to produce a range of spreadsheets • numeracy skills to create and use spreadsheet formulae
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competence may be assessed through: • Interview / Written Test • Observation / Demonstration

Context of Assessment	Competence may be assessed in the work place or in a simulated work place setting.

TOP

Occupational Standard: Hardware and Network Servicing Level I	
Unit Title	**Maintain Inventories of Equipment, Software and Documentation**
Unit Code	**EIS HNS1 07 1221**
Unit Descriptor	This unit defines the competence required to record and store details of software, hardware and technical documentation.

Elements	Performance Criteria
1. Document and update inventory	1.1 ***Hardware inventory*** is maintained that creates a profile or description of each piece of ***equipment*** specification 1.2 ***Software inventory*** and licenses are maintained and updated, as required, particularly when upgrading software 1.3 Storage of user documentation or technical manuals are recorded and organized
2. Store technical documentation	2.1 Action is taken to ensure software, hardware and equipment not in use, stored in a manner as recommended by technical manuals 2.2 Ensure technical documentation is stored securely 2.3 Technical documentation are accessed and disseminated as required by clients

Variable	Range
Occupational Health & Safety (OH&S)	May include but not limited to: Correct posture, lighting, and type of desk, type of monitor, style of chair, typing position, repetitive strain injury prevention, ventilation, light position, correct lifting method, and length of time in front of computer. May also include licensing-related and physical safety considerations such as general electrical safety and cabling, power supply and leads as they apply to computer and peripheral installations.
Hardware inventory	• list of personal computers, networked systems, personal organizers, communications equipment • peripherals may include printers, scanners, tape cartridges, speakers, multimedia kits; keyboard equipment, including mouse, touch pad, keyboard and pens
Equipment	May include but not limited to: • workstations, personal computers, modems or other connectivity devices, printers, hard drives, monitors, switches, hubs, personal digital assistants and other peripheral devices

Software inventory	List of commercial software applications; organization-specific or customized software; word processing, spreadsheet, database, graphic, mail, internet browsers; driver utilities and presentation functionalities with theirs Type, size, version etc...

Evidence Guide	
Critical aspects of Competence	Assessment must confirm the ability to: • accurately and regularly update and maintain the software, equipment and technical documentation inventory according • identify storage and retrieval policy and procedures • software licensing requirements are adhered to according to vendor specifications • inventories are regularly accessed and kept up-to-date • demonstrate workplace documentation and maintenance of technical manual
Underpinning Knowledge and Attitudes	Demonstrates: • Basic understanding of software licensing requirements • Broad knowledge of inventory principles and procedures • Storage of equipment and software • Inventory principles and concept; techniques and procedures
Underpinning Skills	Demonstrates skills to: • perform inventory activities • document and update inventory • store technical documentation • writing reports and documentation • literacy skills in regard to workplace documentation and technical manuals
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level I	
Unit Title	**Identify and Use Network Hand Tools**
Unit Code	**EIS HNS1 08 1221**
Unit Descriptor	This unit describes the performance outcomes, skills and knowledge required to use basic network tools to assist in using a network basically

Elements	**Performance Criteria**
1. Basic network Overview	1.1. General network will be introduced 1.2. Types of networks are identified 1.3. Forms of **ethernet cables** are identified
2. Identify and Uses of basic Network hand-tools	2.1. Identify appropriate ***Network hand tools*** 2.2. Identify appropriate ***Power tools*** 2.3. Uses and functions of network hand tools 2.4. Appropriate use of network hand tools 2.5. Review ***OHS*** requirements for tool use
3. Work with others	3.1 Assistance is sought from workgroup when difficulties arise and addressed through discussions. 3.2 Support is provided to team members to ensure workgroup goals are met. 3.3 Information relevant to work is shared with team members to ensure designated goals are met.

Variable	**Range**
Ethernet cables	• Straight through • Crossover • Rollover

Network hand tools	• Cutter • Crimper • cable stripper • cable testers • multimeter • punch down tool • Toner probe etc…
Occupational Health and Safety (OHS)	OHS precautions and measures may include against: • Physical hazards – impact, illumination, pressure, noise, vibration, temperature, radiation • Chemical hazards – dusts, fibers, mists, fumes, smoke, gasses, vapors Ergonomics • Psychological factors – over exertion/ excessive force, awkward/static positions, fatigue, direct pressure, varying metabolic cycles Physiological factors – monotony, personal relationship, work out cycle • Burglary • Fire • Power accidents

Evidence Guide	
Critical aspects of Competence	Assessment must ensure the ability to – • Identify and safely using of the network hand-tools
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • current network hand-tools(toolkits), such as Cutter, Crimper, cable, stripper, cable testers • how to use network hand-tools, with network cable • organizational guidelines relating to external suppliers and vendors • general understanding of technical systems • current industry-accepted network hand-tools products
Underpinning Skills	Demonstrates skills to: • Use network hand-tools • Technology skills to use hand-tools safely, properly, timely
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and network toolkits, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration

Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level I	
Unit Title	**Access and Use Internet**
Unit Code	**EIS HNS1 09 1221**
Unit Descriptor	This unit defines the competence required to access internet and complete basic web search tasks. It includes finding required information.

Elements	Performance Criteria
1. Access internet	1.1 ***Internet browser*** is opened and a home page of personal choice set up by setting ***internet options***
	1.2 Display/view modes is adjusted to suit personal requirements
	1.3 ***Toolbar*** is modified to meet user and browsing needs
	1.4 Particular site is accessed and retrieved data/download
	1.5 Images are loaded or not loaded depending on modem speed, computer and browser capabilities
	1.6 URL is opened to obtain data and browse link
	1.7 Cookies and history of internet browser are deleted as precaution from virus infection
2. Search internet	2.1 ***Search engines*** are opened and search requirements defined using a range of ***search parameters***
	2.2 Search results are saved and presented as a report according to the information required
	2.3 Bookmarks are created for required web page and saved in associated bookmark folder
	2.4 Page set up options is modified and web page or the required information printed
	2.5 Proxy server is set upped in Internet browser
	2.6 Browser is shut down and exited
	2.7 ***OHS*** and ***netiquette*** principles are observed through the process

3. Organize and Complete Daily Work Activities	*3.1* Work goals and plans are negotiated and agreed with assistance from ***appropriate persons*** 3.2 An understanding of the relationship between individual work goals and plans, and organizational goals and plans is developed 3.3 Workload is planned and prioritized within allocated timeframes 3.4 Tasks are completed within designated time lines and in accordance with ***organizational requirements*** and instructions 3.5 Progress of task is communicated to supervisor or colleagues as required

Variable	**Range**
Internet browser	• Netscape Navigator • Internet Explorer • Mozilla • Chrome • Opera • Galleon • Phoenix • Conqueror • Lynx
Internet options	• configuring of the following options: home page, location of temporary files, privacy level, security level, type of connection and history
Toolbar	• buttons • menus • a combination of both
Search engine	• Northern Light • AOL NetFind • Hotbot • LookSmart • Yahoo • Netscape • Open Text • WebCrawler • Meta Search • Snap • Quest finder • Ask Jeeves • Google • Metacrawler • Alta Vista • Excite

	• Infoseek • Findlink • Lycos • Go To Dot Com • Beaucoup • Search.com • Go2Network • Savvy Search • Profusion • Dogpile • Meta gopher
Appropriate persons	may include but not limited to: • colleagues • other staff members • supervisors, mentors or trainers
Organizational requirements	May include but not limited to: • access and equity principles and practice • anti-discrimination and related policy • business and performance plans • ethical standards • goals, objectives, plans, systems and processes • legal and organization policies, guidelines and requirements • OHS policies, procedures and programs quality and continuous improvement processes and standards
Search parameters	• key words • Logical operators
OHS	• As per company, statutory and vendor requirements. Ergonomic and environmental factors must be considered during the demonstration of this competency • Occupational Health and Safety guidelines related to use of screen based equipment, computing equipment and peripherals, and ergonomic work stations; security procedures; customization requirements
Netiquette	• Is sometimes referred to as web etiquette and is an informal code of manners governing online conduct which may include but is not limited to the use of upper and lower case letters in messages, not spamming other users, not posting commercial messages to newsgroups, learning to lurk before posting, respect for other's time, privacy and bandwidth

Evidence Guide	
Critical aspects of Competence	Assessment must ensure the ability to – • browse the internet

	• search for information
Underpinning Knowledge and Attitudes	Demonstrates knowledge of: • General OHS principles and responsibilities • Makeup and structure of web addresses • Basic technical terminology in relation to reading help files and prompts • Logging procedures relating to accessing a PC • Modem speed, traffic loads in relation to times of accessing the internet • Evaluating and assessing the authority, reliability and authenticity of information • Organizational guidelines on internet and webettique/netiquette • Security, viruses, privacy legislation, copyright • Different types of search engines • Types of software
Underpinning Skills	Demonstrates skills to: • Basic analysis in relation to a limited range of routine areas • Low level decision making in relation to a limited range of routine areas • Problem solving skills in known areas during normal routine • Reading and writing at a level where basic workplace documents are understood • Communication is clear and precise • Interpretation of user manuals • Cultural understanding
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Assessment Methods	Competency may be assessed through: • Interview / Written Test / Oral Questioning • Observation / Demonstration
Context of Assessment	Competency may be assessed in the work place or in a simulated work place setting

TOP

Occupational Standard: Hardware and Network Servicing Level I	
Unit Title	**Apply 5S Procedures**
Unit Code	**EIS HNS1 10 1221**
Unit Descriptor	This unit covers the knowledge, skills and attitude required to apply 5S techniques to his/her workplace. It covers responsibility for the day-to-day operations of the workplace and ensuring that continuous improvements of Kaizen elements are initiated and institutionalized.

Elements	Performance Criteria
1. Prepare for work.	1.1. Work instructions are used to determine job requirements, including method, material and equipment. 1.2. Job specifications are read and interpreted following working manual. 1.3. ***OHS requirements***, including dust and fume collection, breathing apparatus and eye and ear personal protection needs are observed throughout the work. 1.4. ***Tools and equipment*** are prepared and used to implement 5S. 1.5. ***Safety equipment and tools*** are identified and checked for safe and effective operation. 1.6. Kaizen Board (Visual Management Board) is prepared and used in harmony with different workplace contexts.
2. Sort items.	2.1. Plan is prepared to implement sorting activities. 2.2. Cleaning activities are performed. 2.3. All ***items*** in the workplace are identified following ***the appropriate procedures***. 2.4. Necessary and ***unnecessary items*** are listed using the ***appropriate format***. 2.5. ***Red tag*** strategy is used for unnecessary items. 2.6. Unnecessary items are evaluated and placed in an appropriate place other than the workplace. 2.7. ***Necessary items*** are recorded and quantified using appropriate format. 2.8. Performance results are reported using appropriate formats. 2.9. Necessary items are regularly checked in the workplace.
3. Set all items in order.	3.1. Plan is prepared to implement set in order activities. 3.2. General cleaning activities are performed. 3.3. Location/Layout, storage and indication methods for items are decided. 3.4. Necessary tools and equipment are prepared and used for setting in order activities. 3.5. Items are placed in their assigned locations.

	3.6. After use, the items are immediately returned to their assigned locations. 3.7. Performance results are reported using appropriate formats. 3.8. Each item is regularly checked in its assigned location and order.
4. Perform shine activities.	4.1 Plan is prepared to implement shine activities. 4.2 Necessary tools and equipment are prepared and used for shinning activities. 4.3 ***Shine activity*** is implemented using appropriate procedures. 4.4 Performance results are reported using appropriate formats. 4.5 Regular shining activities are conducted.
5. Standardize 5S.	5.1. Plan is prepared and used to standardize 5S activities. 5.2. ***Tools and techniques to standardize 5S*** are prepared and implemented based on ***relevant procedures***. 5.3. Checklists are followed for standardize activities and ***reported*** to ***relevant personnel***. 5.4. The workplace is kept to the specified standard. 5.5. Problems are avoided by standardizing activities.
6. Sustain 5S.	6.1. Plan is prepared and followed to sustain 5S activities. 6.2. Tools and techniques to sustain 5S are discussed, prepared and implemented based on relevant procedures. 6.3. Workplace is inspected regularly for compliance to specified standard and sustainability of 5S techniques. 6.4. Workplace is cleaned up after completion of job and before commencing next job or end of shift. 6.5. Situations are identified where compliance to standards is unlikely and actions specified in procedures are taken. 6.6. Improvements are recommended to lift the level of compliance in the workplace. 6.7. Checklists are followed to sustain activities and report to relevant personnel. 6.8. Problems are avoided by sustaining activities.

Variable	**Range**
OHS requirements	May include, but not limited to: • Legislation/Regulations/Codes of practice and enterprise safety policies and procedures. This may include protective clothing and equipment, use of tooling and equipment, workplace environment and safety, handling of material, use of fire fighting equipment, enterprise first aid, hazard control and hazardous materials and substances.

	• Personal protective equipment is to include that prescribed under legislation/regulations/codes of practice and workplace policies and practices. • Safe operating procedures are to include, but are not limited to the conduct of operational risk assessment and treatments associated with workplace organization. • Emergency procedures related to this unit are to include but may not be limited to emergency shutdown and stopping of equipment, extinguishing fires, enterprise first aid requirements and site evacuation.
Tools and equipment	May include, but not limited to: • Paint • Hook • Sticker • Signboard • Nails • Shelves • Chip wood • Sponge • Broom • Pencil • Shadow board/Tools board
Safety equipment and tools	May include, but not limited to: • Dust masks/goggles • Glove • Working cloth • First aid and safety shoes
Items	May include, but not limited to: • Tools • Jigs/Fixtures • Materials/components • Machine and equipment • Manuals • Documents • Personal items (e.g. Bags, lunch boxes and posters) • Safety equipment and personal protective equipment • Other items which happen to be in the work area
The appropriate procedures	May include, but not limited to: • Steps for implementing 5S (sort, set in order and shine) activities. • Written, verbal and computer based or in some other format.

Unnecessary items	Are not needed for current production or administrative operation and include but not limited to: • Defective or excess quantities of small parts and inventory • Out dated or broken jigs and dies • Worn-out bits • Out dated or broken tools and inspection gear • Old rags and other cleaning supplies • Electrical equipment with broken cords • Out dated posters, signs, notices and memos • Some locations where unneeded items tend to accumulate • In rooms or areas not designated for any particular purpose • In corners next to entrances or exists • Along interior and exterior walls • Next to partitions and behind pillars • Under the eaves of warehouses • Under desks and shelves and in desk and cabinet drawers • Near the bottom of tall stacks of items • On unused management and production schedule boards • In tools boxes that are not clearly sorted
Appropriate format	May include, but not limited to: • All items, necessary and unnecessary items.
Red tag	A format prepared with a red color paper or card which is filled and attached temporarily on the unnecessary items until decision is made. The red tag catch people's attention because red is a color that stands out. So to fill and attach red tag on items, asks the following three questions: • Is this item needed? • If it is needed, is it needed in this quantity? • If it is needed, does it need to be located here?
Necessary items	Are required in the workplace for current production or administrative operation in the amount needed.
Shine activity	May include, but not limited to: • Inspection • Cleaning • Minor maintenance May include, but not limited to: ➢ Tightening bolts ➢ Lubrication and Replacing missing parts
Tools and techniques to standardize 5S	May include, but not limited to: • 5S Job Cycle Charts • Visual 5S • The Five Minute 5S • Standardization level checklist

	• 5S checklist
	• The five Whys and one How approach(5W1H)
	• Suspension
	• Incorporation and Use Elimination
	• 5S slogans
	• 5S posters
	• 5S photo exhibits and storyboards
	• 5S newsletter
	• 5S maps
	• 5S pocket manuals
	• 5S department/benchmarking tours
	• 5S months
	• 5S audit
	• Awarding system
	• Big cleaning day
	• Patrolling system May include, but not limited to:
	  ➢ Top management Patrol
	  ➢ 5S Committee members and Promotion office Patrol
	  ➢ Mutual patrol
	  ➢ Self-patrol
	• Checklist and Camera patrols

Relevant procedures	May include, but not limited to: • Assign 5S responsibilities • Integrate 5S duties into regular work duties • Check on 5S maintenance level • OHS measures such as signage, symbols / coding and labelling of workplace and equipment • Creating conditions to sustain your plans • Roles in implementation
Reporting	May include, but not limited to: • Verbal responses • Data entry into enterprise database • Brief written reports using enterprise report formats
Relevant personnel	May include, but not limited to: • Supervisors, managers and quality managers • Administrative, laboratory and production personnel • Internal/external contractors, customers and suppliers

Evidence Guide

Critical Aspects of Competence	Demonstrates skills and knowledge to: • Discuss how to organize KPT. • Describe the pillars of 5S. • Discuss the relationship between Kaizen elements. • Implement 5S in own workplace by following appropriate procedures and techniques.
Required Knowledge and Attitudes	Demonstrates knowledge of: • Kaizen principle, pillars and concept • Key characteristic of Kaizen • Elements of Kaizen • Wastes/MUDA • Basics of KPT • Aims, benefits and principles of KPT • Stages of KPT • Structure and role of the components of Junior KPT • Concept and parts of Kaizen board • Concept and benefits of 5S • The pillars of 5S • Three stages of5S application • Benefits and procedure of sorting activities • The concept and application of Red Tag strategy • Relevant Occupational Health and Safety (OHS) and environment requirements • Benefits and procedure of set in order activities • Set in order methods/techniques • Benefits and procedure of shine activities • Inspection methods • Planning and reporting methods • Method of Communication • Benefits of standardizing and sustaining 5S • Tools and techniques to sustain 5S • Ways to improve Kaizen elements • Benefits of improving kaizen elements • Relationship between Kaizen elements
Required Skills	Demonstrates skills of: • Participating actively in KPT • Technical drawing • Communication skills • Planning and reporting own tasks in implementation of 5S • Following procedures to implement 5S in own workplace

	• Using sorting formats to identify necessary and unnecessary items • Improving workplace layout following work procedures • Preparing labels, slogans, etc. • Reading and interpreting documents • Observing situations • Gathering evidence by using different means • Recording activities and results using prescribed formats • Working with others • Solving problems by applying 5S • Preparing and using kaizen board • Preparing and using tools and equipment to implement and sustain 5S • Improving Kaizen elements by applying 5S • Standardizing and sustaining procedures and techniques to avoid problems • Procedures to standardizing 5S activities • Analysing and preparing shop layout of the workplace • Standardizing and sustaining checklists
Resources Implication	Access is required to real or appropriately simulated situations, including work areas, materials and equipment, and to information on workplace practices and OHS practices.
Methods of Assessment	Competence may be assessed through: • Interview/Written Test • Observation/Demonstration with Oral Questioning
Context of Assessment	Competence may be assessed in the work place or in a simulated work place setting.

Acknowledgement

We wish to extend thanks and appreciation to the many representatives of business, industry, academe and government agencies who donated their time and expertise to the development of this occupational standard.

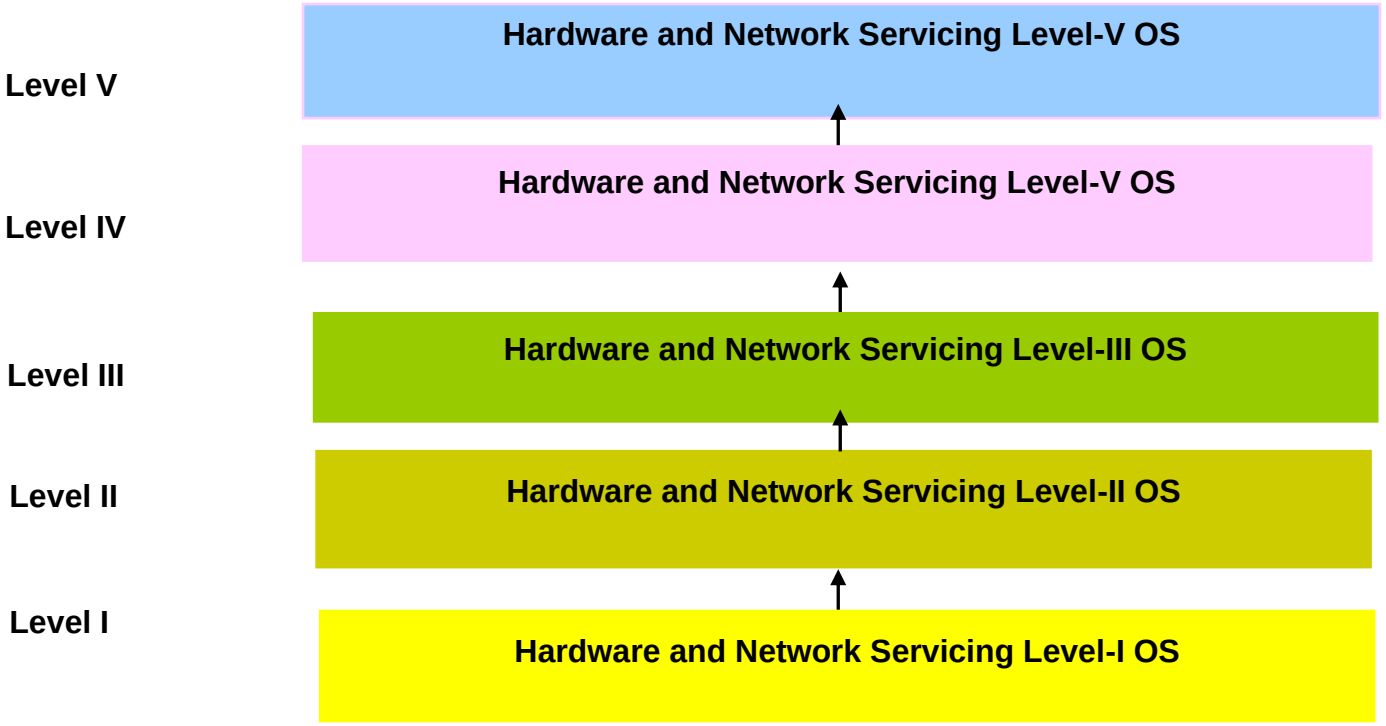
We would like also to express our appreciation to the Staff and Experts of MoFED, Ministry of Education (MoE) and Federal TVET who made the development of this occupational standard possible.

This occupational standard was revised and finalized on December 2021 Adama, Ethiopia.

Sector: Economic Infrastructure

Sub-Sector: Information and Communication Technology

Occupation: Hardware and Network Servicing



List of Experts developed of **Hardware and Network Servicing** Level I – V

No	Name In English	Phone Number	E-mail Address	Region/City
1	Akfete Assefa Hurrisa	0912494821	dirake2121@gmail.com	Adama/Oromia
2	Israel Kifle Addise	0922860138	israelkifle2@gmail.com	Adama/Oromia
3	Edris Fedlu Muzemil	0922976864	edrisfedlu@gmail.com	Addis Abeba
4	Mohammedamin Kabirhussein Abdo	0920081070	mo430ka@gmail.com	Assela/Oromia
5	Yitayal Admie Goshu	0918096684	yitay2007@gmail.com	Addis Abeba
6	Endashaw Girma Dukamo	0926103773	endumulu2009@gmail.com	SNNPR
7	Mululem Hordofa Regasa	0912042074	jimpowerdire@gmail.com	Addis Abeba
8	Abinet Ermias Gobena	0911731227	abinet.erm@gmail.com	SNNPR
9	Amante Tadesse Waldamariam	0923104465	Amantetaddese432@gmail.com	Assela/Oromia
10	Tewodros Sileshi Degesew	0923319916	shurakoyooo@gmail.com	SNNPR