Functional Area: Network Infrastructure & Operation (Security)

1. Title	Implement network access control for internal and external customers to access the network	
2. Code	ITCSNO430A	
3. Range	Network Access Control is an essential part of security which is used to prevent potential snoopers and hackers off a network. In this UoC, it describes the competencies for controlling internal and external customers accessing the network. This means ensuring security with the correct access authority to match the appropriate service which the users are entitled to. The control which being implemented here is at the point where CPE (Customer Premises Equipment) connects to the Access Network. Note: these equipment may be PBX, broadband ADSL (wireless or wireline), etc.	
4. Level	4	
5. Credit	3	
6. Competency		Performance Requirement
	6.1 Possess the knowledge in the subject area	• Critically understand the benefits and reasons for network security, in particular network access control • Experienced with security principles and best practices to protect the network infrastructures and network services • Experienced with risk management principles and be able to identify different network security components • Knowledgeable of CPE security functions that enable suitable access control be configured to gain access to the Access Network • Knowledgeable of regulatory requirements regarding network security • Knowledgeable of health and safety rules and hazards.
	6.2 Implement network access control for internal and external customers to access the network	Be able to: • Acquire access control requirements for a user or a service. For service it usually requires the implementation of a single network control policy. For individual users, different access control will be required depending on the type of services or plans they purchased or jobs to perform (for internal staff) • Determine the authorisation control point e.g. at the server, switch station, firewall, cell point, etc • Consider different types and benefits of different access control, such as “agent based” where the agent is installed at end user’s device, “inline NAC” which all traffics passing through like a firewall, etc • Work with stakeholders (other departments, network control centres, vendors, service roll out teams, customer service, etc.) to determine a best and optimal Access Control • Document the procedures for implementing the controls with details on configuring user’s details into the ACL (Access Control List), including appropriate access permission at appropriate switches, equipment, devices and servers, firewalls, etc. • Perform the implementation of access control and test the control with appropriate warnings/alerts when irregularities are detected • Package the results of the test and present to stakeholders for job signoff or approval
	6.3 Exhibit professionalism	• Follow the heath and safety guidelines of the organisation • Always take into consideration and strike a proper balance among all related technological, environmental and legal factors

7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: i. determine the level of access security requirements to be implemented ii. communicate effectively with stakeholders to formulate a suitable access control at appropriate point of access authorisation iii. document the access control implementation plan, in an easy to understand format, and perform the implementation iv. test to ensure the access control performed as expected v. demonstrate that the implementation was satisfactorily completed with test results, and with stakeholders' approval
Remark	