Functional Area: Network Infrastructure & Operation (Security)

1. Title	Define network security policies	
2. Code	ITCSNO529A	
3. Range	Without a security policy, the availability of the network can be compromised by hackers, fraud users, and poor workmanship such as incorrect configuration of routers and switching equipment. It will create problems for network support teams and certainly business will be affected. The policy begins with assessing the risk to the network and building a team to respond. This UoC describes the competencies for defining network policies.	
4. Level	5	
5. Credit	3	
6. Competency		Performance Requirement
	6.1 Possess the knowledge in the subject area	• Possess extensive knowledge of the organisation's policy formulation mechanism and business needs. • Knowledgeable of the organisation's security policies • Possess extensive knowledge of telecom regulatory requirements, particularly security related • Experienced with the network infrastructure and all the services that it supports • Possess extensive knowledge of security principles and best practices • Expert in analysing and identifying various security risks such as possible method of attacks on signalling layer, database of subscribers, network elements, gateways, frauds, and service interruptions, etc. • Knowledgeable of health and safety rules and hazards.
	6.2 Define network security policies	Be able to: • Perform security risk analysis of the network by identifying assets, threats and vulnerabilities of the network infrastructure and its components • Rank the different assets in order of importance for the business • Identify threats and risks to the organisation's assets, such as: unauthorised access/use of resources (authentication), Denial of Service (availability), leakage of information (confidentiality), corruption/unauthorised change of data (integrity), natural disasters. etc • Evaluate different alternatives to handle the risks • Group the risks into categories in terms of: must be minimised/eliminated, should be minimised/eliminated or acceptable • Plan the appropriate security mechanism (what to implement, how to monitor the effectiveness) conforming to the organisation's policies, for the 3 risk categories • Document the security policies with review schedules • Distribute policy to appropriate stakeholders for implementation and enforcement such as: security officers, NOC (Network Operation Centre), network engineers, service desk, etc
	6.3 Exhibit professionalism	• Ensure the policy is written in a manner that can be understood by non technical person and comply with the organisation standards • 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. comprehend the organisation’s security policies and apply these security needs to the formulation of network security policy ii. identify the risks and categorise the type of risks associated with the network iii. formulate suitable risk mitigation procedures to handle different categories of risk iv. effectively transform the mitigation procedures to network security policies v. disseminate the policies to stakeholders to comprehend and take appropriate action such as: approval, signoff, implementation and enforcement
Remark	