|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TSC Category** | Development and Implementation | | | | | |
| **TSC Title** | Network Security | | | | | |
| **TSC Description** | Design and configure network systems to ensure the integrity of network infrastructure through the use of appropriate protection, detection and response mechanisms | | | | | |
| **TSC Proficiency Description** | **Level 1** | **Level 2** | **Level 3** | **Level 4** | **Level 5** | **Level 6** |
|  |  | **ICT-DIT-3024-1.1** | **ICT-DIT-4024-1.1** | **ICT-DIT-5024-1.1** |  |
|  |  | Install, configure and test network security | Manage network security throughout a network | Design and implement wireless network security |  |
| **Knowledge** |  |  | * Security requirements of the organisation * Virtual Private Network (VPN), types, functions and operation, issues, bandwidth and dynamic security environment * Configuration of routers and switches * Hardware and software security products, features and capabilities * Network protocols and operating systems * Security perimeters, functions, protocols, standards and data encryption | * Infocomm Technology (ICT) networks and their configuration * Types of network attacks, vulnerabilities and related weaknesses of installed infrastructure * Types and techniques of network security measures * Network security implementation risk management plans and procedures | * Configuration, verification and troubleshooting procedures relating to router operation and routing and virtual local area network (VLAN) switching and inter-switching components * iDevice Operating System (iOS) and Internet Protocol (IP) networking models * Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) security protection * Threat mitigation strategies * Wireless Local Area Networks (WLAN) regulations, standards and certifications * WLAN network security technology, network topologies, architectures and elements, and networking protocols |  |
| **Abilities** |  |  | * Identify and analyse network security threats and vulnerabilities * Propose recommendations to management to address network security deficiencies * Implement perimeter security, network hardening measures and authentication and user account controls according to identified deficiencies and organisational asset security requirements * Design and conduct testing to verify the key functions and performance measures of network security * Debug network security according to test results * Review logs and audit reports to record security incidents, intrusions and attempts | * Identify threats to network security * Analyse security risks * Determine organisational assets that require protection * Create risk management plans to mitigate risks * Define planning, building and management phases for network security design * Develop security measures for network components * Design auditing and incident response procedures * Document security incidents * Implement configurations aligned with incident response procedure design | * Conduct research and evaluate organisational, regulatory and security policies used to benchmark acceptable network security standards * Produce plans with security solution documentation for future growth and security needs * Design, implement and test guess access services * Configure WLAN controller authorisation, anchor and internal controllers * Design and configure authentication of clients and management frame protection on clients and controllers * Design, implement and test the integration of wireless network with organisational network admission and controls systems * Evaluate and plan secure wireless connectivity services * Evaluate end-to-end security solutions to assess how they integrate with the planned wireless systems * Configure and test the WLAN controllers for wired and wireless intrusion prevention and detection system security protection |  |
| **Range of Application** |  | | | | | |