SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY
TECHNICAL SKILLS & COMPETENCIES (TSC) REFERENCE DOCUMENT

TSC Category	Operations and User Support					
TSC Title	Security Administration					
TSC Description	Administer, configure and update of security programmes and mechanisms, including the application of system patches to ensure that enterprise assets are adequately protected against threats. This also includes the authorisation, management and monitoring of access control permissions and/or rights to various IT facilities					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		ICT-OUS-2012-1.1	**ICT-OUS-3012-1.1**	**ICT-OUS-4012-1.1**		
		Run system diagnostic tools, and install and update simple, basic security programmes, virus protection and system patches	Administer, configure and troubleshoot security programmes and mechanisms, and analyse impact of patches and updates on system and networks	Plan the administration and technical operationalisation of security programmes, and investigate security breaches in information, system and network access		
Knowledge		• Basic concepts and processes of system administration • Available system updates and patches • Use of system and network diagnostic tools • Configuration procedures • Preventative maintenance procedures • Access rights management processes • Indicators of security and access anomalies	• Complexities in system and network administration • Methods of configuration for a range of software and hardware • Security software troubleshooting techniques • Principles of access rights and permissions • Process of investigation for security breaches and unauthorised access	• End-to-end security administration processes • Range of tools and techniques to enhance website security • Emerging security issues and threats • Security weaknesses of installed infrastructure • Key principles of user access management and control • Implications of various levels of user access • Diagnosis of security breaches		
Abilities		• Administer security programmes and updates • Install standard system patches to maintain a secure system environment • Run system and network diagnostic tools according to specifications	• Administer new and complex security programmes for the organisation • Analyse the impact of patches and updates on current system • Perform non-standard system /and network administration and configuration of security mechanisms	• Facilitate the administration and technical operationalisation of security programmes • Plan the installation of relevant hardware, software and operating systems to protect the organisation against threats		

		• Modify system configuration as indicated by the system diagnostic tools • Scan the system and networks periodically to check and maintain virus protection • Apply basic access rights and permissions on a day to day basis, according to established protocols • Follow prescribed protocols to assess rules, access controls and configurations to report suspected anomalies • Assist in investigation of issues relating to security systems and access controls	• Configure authentication software and features of network devices as required to protect against security threats • Perform post-implementation troubleshooting of security software • Assist users in defining and clarifying their access rights and privileges • Coordinate complicated access control rights, permissions and escalated issues • Investigate unauthorised access incidents according to established procedures	• Update security administration plans and relevant personnel in view of new and emerging cybersecurity policies and security threats • Manage security administration processes to ensure requests, activities and updates are handled according to internal protocols • Establish access control rules and permissions, aligned with organisational priorities and security parameters • Facilitate organisation-wide communication of access control rules, rights and permissions • Plan monitoring and control methods for managing user access • Grant permissions for role-based access requests, based on their compliance with organisational standards and procedures • Investigate significant security breaches in information and system or network access and recommend required action		
Range of Application						