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

TSC Category	Operations and User Support					
TSC Title	Cyber Forensics					
TSC Description	Develop and manage digital forensic investigation and reporting plan which specifies the tools, methods, procedures and practices to be used. This includes the collection, analysis and preservation of digital evidence in line with standard procedures and reporting of findings for legal proceedings					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		ICT-OUS-2002-1.1	**ICT-OUS-3002-1.1**	**ICT-OUS-4002-1.1**	**ICT-OUS-5002-1.1**	**ICT-OUS-6002-1.1**
		Scan, retrieve and preserve digital evidence from various sources, following authorised protocols	Coordinate the collection and preservation of evidence and analyse forensic evidence to draw inferences	Develop a digital forensic investigation plan, and integrate analysis of evidence, outlining key conclusions, insights and recommendations	Establish digital forensic investigation policies and protocols for the organisation, and manage multiple investigations	Define new cyber forensics tools, techniques and methodologies and lead cyber forensics investigations on an international scale
Knowledge		• Types of data devices and storage • Features of the different type of data services storage • Types types of computer, network and mobile evidence • Computer forensic hardware and software tools • Procedures used to acquire, preserve and maintain integrity of evidence • Safe handling techniques to prevent contamination or tampering of evidence for different IT systems	• Potential internal and external data sources • Range of analytical techniques to examine digital evidence • Broad range of computer, network and mobile forensic tools and techniques • Statistical analysis procedures used to identify trends • Legal principles and regulations in relation to forensic investigations	• End-to-end process and procedures in a forensics investigation • Critical milestones and touchpoints in a forensics investigation • Emerging and specialised forensic tools, solutions and methodologies • Changes and updates to regulatory or legal requirements • Implications of regulatory and legal parameters on forensic investigations	• Evolving trends in forensic investigation • New and emerging trends in the Infocomm Technology or related fields • Impact and consequences of forensics investigation policies and protocols on the organisation	• Cyber forensics tool development • Cyber forensics process development • International considerations and implications of cyber forensics investigations and activities
Abilities		• Access evidence from electronic devices using various forensic tools • Extract digital evidence from various sources, following authorised protocols • Use forensic tools to back up and preserve	• Monitor a range of internal and external data sources to identify relevant information to incident at hand • Coordinate the collection and preservation of digital evidence	• Develop a digital forensic investigation plan, including the tools, processes and methodologies to be used • Assess suitability of new and emerging forensic	• Establish digital forensic investigation policies and standards for the organisation • Develop protocols and Standard Operating Procedures (SOP) for investigation procedures including guidelines for	• Chart direcrtion for new cyber forensics techniques and methodologies • Establish cyber or digital forensic tools for adoption

		evidence to prevent tampering • Store original and copied evidence in safe environments with limited access	• Examine digital evidence to identify patterns and suspicious or unauthorised activity • Analyse forensic evidence and document inferences • Analyse patterns and correlations of events data to draw conclusions • Present digital forensic findings in an appropriate format which complies to legal and company regulations	tools, given investigation requirements • Determine the key tasks, timelines, milestones and accountabilities for a specific forensic investigation • Perform robust investigation activities and forensic analysis to determine the underlying causes and effects of incidents • Lead forensic investigations, involving interaction with large data sets, operating systems or networks • Review multi-source evidence and conclusions drawn in light of broader trends and contextual considerations • Develop a report to documents the findings, conclusions and recommendations	interviews, data handling, surveillance etc. • Manage plans for multiple digital forensic investigations and large-scale forensic investigation activities for forensic teams • Present reports and outcomes in significant investigations or legal proceedings	• Review robustness of protocols and SOPs for investigation procedures • Lead cyber forensics investigations on an international scale
Range of Application						