SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY
SKILLS MAP – FORENSICS INVESTIGATOR

Sector	Infocomm Technology
Track	Cyber Security
Sub-track	Forensics Investigation
Occupation	ICT Security Specialist
Job Role	**Forensics Investigator**
Job Role Description	The Forensics Investigator is responsible for the investigation processes after a cyber-threat or incident. He/She is responsible to collect and analyse the threat data from the affected systems. He is also responsible for performing the forensics investigation and determining the root cause of cyber-attacks. He is familiar with different types of threats, cyber security standards, protocols and frameworks, and acts in accordance with the Cyber Security Act 2018. He is knowledgeable of hardware and software applications to analyse threat data from various sources. The Forensics Investigator is diligent and takes an analytical approach to perform analyses and uncover insights. He is skilled in synthesising trends and insights, and is confident in putting forth creative mitigation plans and solutions to mitigate security incidents.

	Critical Work Functions	**Key Tasks**	**Performance Expectations**
Critical Work Functions, Key Tasks and Performance Expectations	**Collate threat data post-cyber attack**	Collect information from affected stakeholders and document the impact of the cyber-attack	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
		Scan IT systems to retrieve information from storage and other electronic devices	
		Collect and decrypt threat data from affected IT systems	
		Perform cross analysis of threat data with existing threat database to classify the threat data	
	Oversee forensic investigations	Conduct forensic analysis and investigations to determine the causes of security incidents	
		Distil key insights and impact from analyses of security incidents	
		Contain the impact of security incidents	
		Prepare investigative reports detailing incident findings, analysis and conclusions	
		Update threat database based on investigation findings	
		Provide insights and recommendations to affected stakeholders on post investigation findings and cyber-attack mitigation strategies	

	Technical Skills and Competencies		**Generic Skills and Competencies**	
Skills and Competencies	Cyber Forensics	Level 3	Communication	Intermediate
	Cyber Risk Management	Level 4	Creative Thinking	Intermediate
	Emerging Technology Synthesis	Level 3	Problem Solving	Intermediate
	Failure Analysis	Level 3	Sense Making	Intermediate
	Network Security	Level 3	Teamwork	Intermediate
	Security Administration	Level 3		
	Security Assessment and Testing	Level 3		
	Stakeholder Management	Level 3		
	Threat Analysis and Defence	Level 3		
	Threat Intelligence and Detection	Level 3		

Programme Listing	For a list of Training Programmes available for the ICT sector, please visit: www.skillsfuture.sg/skills-framework/ict

The information contained in this document serves as a guide.