SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY SKILLS MAP – INCIDENT INVESTIGATOR				
Sector	Infocomm Technology			
Track	Cyber Security			
Sub-track	Incident Response			
Occupation	ICT Security Specialist			
Job Role	**Incident Investigator**			
Job Role Description	The Incident Investigator conducts complex analysis to investigate causes of intrusion, attack, loss or breach occurring in an organisation. He/She identifies and defines cyber threats and root causes. He develops reports that detail incident timeline, evidence, findings, conclusions and recommendations. He is responsible for managing cyber incidents and resolving the incidents in a timely manner. He prepares reports, communicates findings to senior stakeholders, and recommends corrective actions to prevent and mitigate internal control failures. He is required to be on standby with on-call availability with varied shifts including nights, weekends and holidays. He is familiar with cyber security standards, protocols and frameworks, and works in compliance with the Cyber Security Act 2018. He is knowledgeable in using various cyber security tools and techniques to resolve incidents. The Incident Investigator is detail-oriented and adopts a critical and systematic approach in conducting investigations and analyses. He views issues from multiple perspectives and actively communicates his thoughts and engages with other team members.			
Critical Work Functions, Key Tasks and Performance Expectations	**Critical Work Functions**	**Key Tasks**	**Performance Expectations**	
	Develop and implement cyber incident response strategy	Develop approaches to combat cyber threats and mitigate risks to information systems assets	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore	
		Develop guidelines to perform incident response strategies and policies		
		Implement processes and guidelines to perform incident response protocols, analyse data, and create incident reports		
		Implement mechanisms to improve cyber security measures and incident response times		
	Manage cyber security incidents	Handle responses to cyber security incidents		
		Lead the recovery of contained cyber security incidents, following established processes and policies		
		Utilise appropriate cyber incident management techniques to resolve challenges		
	Oversee cyber threat analysis	Collect, analyse and store cyber threat intelligence information		
		Analyse past cyber-attacks to draw insights and implications on the organisation		
		Scrutinise vulnerabilities within systems that may pose cyber security risks		
		Recommend ways to enhance the resilience and security of IT systems		
		Propose mitigation techniques and countermeasures to ensure cyber threats are kept at a minimum		

Skills and Competencies	**Technical Skills and Competencies**		**Generic Skills and Competencies**	
	Cyber Forensics	Level 3	Communication	Intermediate
	Cyber and Data Breach Incident Management	Level 3	Creative Thinking	Intermediate
	Cyber Risk Management	Level 4	Problem Solving	Intermediate
	Security Assessment and Testing	Level 3	Sense Making	Intermediate
	Stakeholder Management	Level 3	Teamwork	Intermediate

Effective date: January 2020, Version 2.1

	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.

Effective date: January 2020, Version 2.1