SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY
SKILLS MAP – ASSOCIATE SECURITY ANALYST

Sector	Infocomm Technology
Track	Cyber Security
Occupation	ICT Security Specialist
Job Role	**Associate Security Analyst**
Job Role Description	The Associate Security Analyst supports security systems, operations administration, monitoring and maintenance of cyber security systems and applications. He/She monitors security alerts and events. He collects and documents information based on established practices and supports the preparation and publishing of security advisories. He assists with the analysis of security-related information and events, escalation of incidents for validation and remediation. 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 is required to act in accordance with the Cyber Security Act 2018. He is knowledgeable in using various cyber security tools and techniques to monitor and resolve incidents. The Associate Security Analyst is alert and vigilant in performing monitoring activities and is able to analyse and resolve security-related issues critically. He communicates clearly in his interactions with others and coordinates effectively with his team to perform security operations.

	Critical Work Functions	**Key Tasks**	**Performance Expectations**
Critical Work Functions, Key Tasks and Performance Expectations	**Monitor cyber security systems**	Perform cyber security monitoring activities on IT systems and applications	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
		Categorise security incidents and breaches that occur	
		Track and react to security monitoring alerts	
		Compile reports on the performance of security operations for management reporting	
	Maintain cyber security operations	Assist with the implementation of agreed security system changes and maintenance routines	
		Assist in the implementation of new cyber security programs	
		Assist with conducting vulnerability and penetration assessments	
		Assist in aligning cyber security systems with established service agreement standards	
		Maintain documentation of all maintenance procedures and tests on cyber security systems	
	Respond to cyber security queries	Assist in responding to cyber security issues	
		Assist in forensic threat investigations	
		Assist with resolution of security-related issues	
		Assist with simulation of user problems to identify drawbacks of cyber security systems	
		Recommend modifications to cyber security systems to address issues	
		Maintain logs of cyber security incidents	
	Facilitate cyber security compliance	Assist with the implementation security policies, standards and procedures	
		Educate users on cyber security policies, standards and practices	
		Identify improvement areas to existing security policies and procedures	
		Monitor third party compliance with organisational cyber security policies, standards and procedures	
		Monitor users' adherence to cyber security policies, standards and procedures	

	Optimise cyber security system performance	Assist with piloting of new cyber security tools, technologies, and processes	
		Assist with installation of new cyber security related hardware and software	
		Assist with security system testing and ongoing optimisation or changes such as scheduled upgrades and updates	
		Maintain documentation of all optimisation activities	
		Recommend security products, services and/or procedures	
		Propose improvements to IT operational processes, procedure manuals, and documentation	
Skills and Competencies	**Technical Skills and Competencies**		**Generic Skills and Competencies**	
	Business Needs Analysis	Level 2	Communication	Basic
	Cyber and Data Breach Incident Management	Level 2	Creative Thinking	Basic
	Cyber Forensics	Level 2	Problem Solving	Intermediate
	Infrastructure Support	Level 3	Sense Making	Intermediate
	Network Administration and Maintenance	Level 1, Level 2	Teamwork	Intermediate
	Problem Management	Level 3		
	Security Administration	Level 2		
	Security Assessment and Testing	Level 2		
	Security Education and Awareness	Level 3		
	Security Programme Management	Level 3		
	Stakeholder Management	Level 2		
	Threat Analysis and Defence	Level 3		
	Threat Intelligence and Detection	Level 2		
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.