SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY SKILLS MAP – SENIOR SECURITY ENGINEER/SECURITY ENGINEER					
Sector	Infocomm Technology				
Track	Cyber Security				
Sub-track	Security Design and Engineering				
Occupation	ICT Security Specialist				
Job Role	**Senior Security Engineer/Security Engineer**				
Job Role Description	The Senior Security Engineer/Security Engineer designs, develops and implements secure system architectures. He/She embeds security principles into the design of system architectures to mitigate the risks posed by new technologies and business practices. He designs artefacts, spanning design, development and implementation, into enterprise systems that describe security principles and how they relate to the overall enterprise system architecture. He performs routine activities related to the periodic review and audit activities of infrastructure security systems and maintains documentation of security standards and procedures. He is well versed with cyber security standards, protocols and frameworks, and works in compliance with the Cyber Security Act 2018. He is knowledgeable of various application and hardware technologies and services. The Senior Security Engineer/Security Engineer is structured and systematic in his approach to designing and implementing secure system architectures. He is articulate and works well with his team and other stakeholders.				
Critical Work Functions, Key Tasks and Performance Expectations	**Critical Work Functions**	**Key Tasks**	**Performance Expectations**		
	Develop architecture requirements and maintain oversight	Design security controls and systems in alignment with security guidelines	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore		
		Assist in the testing and evaluation of new security technologies and controls			
		Recommend security products, services and procedures to enhance system architecture designs			
		Document the design, operation, use, and expected outputs of new systems			
		Conduct research on modern security software architectures and network architecture design best practices			
	Implement security systems	Implement new enterprise security architecture, technologies and enhancements			
		Identify techniques to scale up and automate security infrastructure and processes			
		Resolve issues that arise in implementation of new security systems			
		Monitor security systems for strengths and weaknesses and propose improvements to address weaknesses			
	Manage security systems	Oversee the maintenance of security systems, platforms and associated software			
		Develop and implement custom disaster recovery drills and simulation tests on existing systems			
		Assist in the resolution of identified problems and incidents			
Skills and Competencies	**Technical Skills and Competencies**			**Generic Skills and Competencies**	
	Business Needs Analysis	Level 3		Communication	Intermediate
	Cyber and Data Breach Incident Management	Level 3		Computational Thinking	Intermediate
	Cyber Risk Management	Level 4		Problem Solving	Intermediate
	Emerging Technology Synthesis	Level 3		Sense Making	Intermediate
	Infrastructure Design	Level 3		Teamwork	Intermediate

Effective date: January 2020, Version 2.1

	Network Security	Level 4	
	Security Administration	Level 3	
	Security Architecture	Level 3	
	Security Governance	Level 4	
	Security Programme Management	Level 3	
	Strategy Implementation	Level 4	
	Strategy Planning	Level 4	
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