Specification of Competency Standards for ICT Operation and Support
Unit of Competency

Functional Area: Security Support

Title	Administer perimeter firewall
Code	107890L3
Range	This unit of competency applies to IT personnel who administer the organisation's network security; particularly the perimeter firewall which protects the organisaton internal network from the external network. The administering tasks of these IT personnel include but not limited to: maintain firewall filtering rules, monitor security logs, perform maintenance of the firewall, ensure the firewall is always on, etc.
Level	3
Credit	3

Competency	Performance Requirements
	1. Knowledge for administering perimeter firewall:
	• Possess good communication and interpersonal skills
	• Possess detailed knowledge of network security and different risks
	• Possess detailed knowledge of firewall concept
	• Possess good knowledge of operating firewall and monitoring equipment
	• Understand the organisation's network security requirements and policies
	• Well updated with network security threats, technologies and trends
	2. Administer perimeter firewall
	• Perform regular monitoring of perimeter firewall to ensure it is fully functioning.
	• Perform reconfiguration of settings when required. Configuration settings that affect security of the network must follow the organisation guideline and procedures before action
	• Manage firewall filtering rules to match the organisation's and process users needs, including:
	  • Create new rules
	  • Amend existing rules
	  • Remove redundant and conflicted rules
	• Regularly review the list of filtration rules to verify rules still effective and are being used. Cleanup unused rules to maintain efficiency and performance of the firewall
	• Regularly monitor and review access logs to ensure no security breach or any irregularities. When irregularities found, escalate to supervisor and investigate
	• Assist supervisor to review operation procedures, such as "filtration rule change" requests
	• Perform backup of firewall database after any change of settings or filtering rules
	• Document all changes (configuration, rules) and actions performed on the firewall in accordance to the organisation standards
	3. Exhibit professionalism
	• Ensure perimeter protection complied with the organisation guideline
	• Exhibit security attitude but balancing the need of users with the security need when administering the perimeter security
	• Well converse with industry network security best practices

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Set up the firewall that matches the organisation business requirements and securely protect the internal network from external environment • Use the firewall monitoring facilities or security log to monitor irregular activities • Follow the orgnaisation's procedures to document all changes and actions made on the firewall
Remark	