Unit of Competency

Functional Area: Security Support

Title	Create and maintain user accounts on server
Code	107885L2
Range	This unit of competency applies to support personnel who administer the organisation's servers. A very important task for the administrator or the support personnel of servers is to create accounts of users that are allowed to access the system's resource. This UoC assumes servers are standalone and not in directory service environment
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge for creating and maintaining user accounts on server • Possess system troubleshooting skills • Possess good knowledge of system logs • Possess good knowledge of common server operating systems • Possess good knowledge of operating system's access control • Possess basic knowledge of information security • Possess knowledge of the organisation's user security procedures and guidelines

Unit of Competency

Functional Area: Security Support

Competency	2. Create and maintain user accounts on server
	• Determine the needs of the accounts on server, such as:
	  • The role of the user (user, administrator, operator, etc.)
	  • Which server, if there are more than one
	  • Personal folder for the user
	  • Access to server resources
	  • Application settings
	  • Access rights
	• Login to server with administrative account to create the new account and follow the organisation guidelines to setup security settings for the account based on the role of the user. Settings include but not limited to the following:
	  • Security role of the account
	  • Directory and file permissions
	  • Password length
	  • Change password requirements and duration
	• Set temporary password and set user must-change-password on first login
	• Inform the user of new account details
	• Regularly use system tools or third party tools to determine security and usage of accounts, such as but not limited to the following:
	  • Accounts involved with unusual activities
	  • Attempt to access unauthorised resources
	  • Accounts locked out
	  • Unused accounts
	• Handle unusual account activities in accordance to the organisation guideline, such as escalating to supervisor
	• Verify unused accounts and follow the organisation procedures to perform clean-up activities, such as remove account, revoke permission, etc.
	• Document and record all actions performed on user account in accordance with the organisation guidelines
	3. Exhibit professionalism
	• Apply system administrator ethics and exercise due diligence when administering user accounts on servers
	• Exhibit security attitude but balance the needs of users with the organisation security needs when administering system user accounts, as well as securing the server

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Understand the needs for creating new accounts • Use appropriate system tools to create accounts, perform correct configurations, setup correct access rights to server resources and provide sufficient details and guidance to user that enabling him/her to access the server • Monitor account usage and account irregular activities and take corrective actions to maintain accounts current and secured on the server
Remark	