# Specification of Competency Standards for ICT Operation and Support

## Unit of Competency

### Functional Area: Security Support

<table>
<thead>
<tr>
<th>Title</th>
<th>Configure user access control on server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td>107886L3</td>
</tr>
</tbody>
</table>

### Range

This unit of competency applies to support personnel who administer the organisation’s servers. To access resources on a server the user will need appropriate access rights which administrator will need to configure. Access control in modern servers has pre-configured access control in form of different roles or via traditional access rights.

<table>
<thead>
<tr>
<th>Level</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit</td>
<td>3</td>
</tr>
</tbody>
</table>

### Competency

**Performance Requirements**

1. **Knowledge for configuring user access control 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

2. **Configure user access control on server**
   - Determine what role the user is allocated by the organisation, for example:
     - Administrator
     - Backup operator
     - Application administrator
     - Read only analyst
   - Use server management tools to assign the role to the user’s account
   - Determine resource access permitted for the user, such as but not limited to the following:
     - Local logon
     - Internet access
     - Remote logon
   - Use server tool to configure user accounts with allowed access
   - Create a check list of access control setting for each shared resources and/or object, such as but not limited to the following:
     - Printers
     - Folders
     - Files
     - Applications
   - Configure the allowed access and level of access (Read, Write, Execute, etc.) to each object and shared resource
   - Document and record all user access setting and configuration for reference

3. **Exhibit professionalism**
   - Comply system administrator ethics and exercise due diligence when administering user accounts and access control on servers
   - Exhibit security attitude but balance the needs of users with the organisation security needs when setting user access control as well as protecting the server
## Functional Area: Security Support

<table>
<thead>
<tr>
<th>Assessment Criteria</th>
<th>The integrated outcome requirements of this UoC are the abilities to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Determine and setup the role of the user that matches his/her access on the server</td>
</tr>
<tr>
<td></td>
<td>• Identify all the individual objects, shared resources on the server which the user requires access to</td>
</tr>
<tr>
<td></td>
<td>• Setup and configure correctly the user’s access control on the server</td>
</tr>
</tbody>
</table>

| Remark |