Unit of Competency

Functional Area: Security Support

Title	Administer basic network security
Code	107887L3
Range	This unit of competency applies to support personnel who administer the organisation’s network security on their regular day to day duties. The duties include supporting users request for network access and ensuring the network is protected in accordance with the organisation’s requirements. The organisation network infrastructure, in this context, is a small or simple type which may consists of one perimeter firewall, WAN Internet router, wireless LAN Access Point (AP) for mobile clients, one central switch and a number of group switches with hosts (workstations or servers) connected. Network services may include: file service, network printing, Virtual Private Network (VPN) or remote access, etc.
Level	3
Credit	3
Competency	Performance Requirements 1.Knowledge for administering basic network security: • Possess good communication and interpersonal skills • Possess network troubleshooting skills • Understand system and network monitoring equipment logs • Able to operate the organisation network devices • Possess broad knowledge network function and features of network devices • Possess knowledge of threats and the importance of network security • Possess knowledge of the organisation’s network security procedures and guidelines

Unit of Competency

Functional Area: Security Support

<table>
<tr><td>Competency</td><td>2. Administer basic network security
<ul>
<li>Comprehend the organisation’s network infrastructure, daily activities list and security policies</li>
<li>Determine the network security status including but not limited to the following:
<ul>
<li>Network devices are operating normally via visual check, including: power lights are on, cables are not loose</li>
<li>Review monitoring and system logs and audit reports to ensure no unauthorised access or irregularities</li>
<li>Ensure Internet security (antivirus, anti-spyware) filtering/detection systems are still effective and up to date</li>
<li>When irregularities are detected, analyse, evaluate and handle irregularities in accordance with the organisation’s procedures, seek assistance if necessary. Actions may include:
<ul>
<li>Adjust firewall rules,</li>
<li>Change wireless AP security passwords.</li>
<li>Segregate guest mobile users, if necessary</li>
<li>Train users on network security functions</li>
<li>Adjust access control on network resources</li>
<li>Report irregularities to supervisor</li>
</ul></li>
</ul></li>
<li>Facilitate user’s request to define and configure suitable level of network access on network controlling devices but ensure it conformed to the organisation security specifications</li>
<li>Regularly perform security patches and updates of network devices when required</li>
<li>Regularly review and evaluate the network security to ensure it is well protected and conforms to the organisation needs and complied with regulatory requirement, if any</li>
<li>Document actions/changes to the network in accordance with the organisation’s procedures. Consult with colleagues and supervisors when required</li>
</ul>
3. Exhibit professionalism
<ul>
<li>Ensure network security complied with the organisation and regulatory requirements</li>
<li>Exhibit security attitude but balancing the need of users with the security need when administering the network security</li>
<li>Well converse with industry network security best practices and keep updated with trends of network security</li>
</ul></td></tr>
<tr><td>Assessment Criteria</td><td>The integrated outcome requirements of this UoC are the abilities to:
<ul>
<li>Analyse security logs and reports to determine security irregularities</li>
<li>Handle and rectify network security irregularities in accordance with the organisation procedures</li>
<li>Set the correct level of network access for users in accordance with the organisation procedure</li>
</ul></td></tr>
<tr><td>Remark</td><td></td></tr>
</table>