

**Specification of Competency Standards**  
**for the Logistics Industry**  
**Unit of Competency**

Functional Area - Smart Logistics

Title	Manage network security
Code	LOCUEL503B
Range	This unit of competency is applicable to logistics service providers. Practitioners should be able to manage network security effectively.
Level	5
Credit	3 (For Reference Only)
Competency	<p>Performance Requirements</p> <p>1. Possess the knowledge of network security</p> <ul style="list-style-type: none"> <li>• Know about the principle of network security</li> <li>• Understand the business operations of logistics related industries</li> <li>• Understand company procedures and requirements</li> <li>• Understand the legal requirement and obligation of the company and their users</li> </ul> <p>2. Identify threats</p> <ul style="list-style-type: none"> <li>• Implement risk analysis of security threats faced by company network</li> <li>• Evaluate and identify internal and external threats to network such as hackers, eavesdropping and viruses</li> </ul> <p>3. Identify appropriate controls</p> <ul style="list-style-type: none"> <li>• Plans for cost effective improvements to network security are presented to management for approval and authorisation</li> <li>• Present external or intra network security devices and controls such as firewalls to management for approval</li> <li>• Identify controls to be installed in the network to manage elements such as user access or hackers, eavesdropping and viruses</li> </ul> <p>4. Establish effective network security plan</p> <ul style="list-style-type: none"> <li>• Install and configure approved equipment and controls to provide required levels of security</li> <li>• Evaluate the effectiveness of network security plan on a regular basis</li> <li>• Provide recommendations for additional equipment and updates to maintain security integrity</li> </ul>
Assessment Criteria	<p>The integrated outcome requirements of this unit of competency are:</p> <ul style="list-style-type: none"> <li>• Capable of assessing and identifying threats faced inside and outside the network;</li> <li>• Capable of recommending cyber security improvement plans based on cost-effectiveness and required security levels; and</li> <li>• Capable of evaluating the effectiveness of the cyber security plan, and make recommendations for installing additional equipment and updating the network for maintaining security integrity</li> </ul>
Remark	