Specification of Competency Standards
for the Travel Industry
Unit of Competency

Functional Area - Information technology application and support

Title	Master computer virus detection and prevention technology
Code	110746L4
Range	This unit of competency involves IT skills. Practitioners should be able to master computer virus detection and protection techniques to handle daily defence and system updates, and prepare emergency response measures
Level	4
Credit	5 （For Reference Only）

Competency	Performance Requirements
	
	1. Master the basic knowledge of computer viruses
	
	• Understand the basic operation principles, operation mechanisms, classifications and structures of computer viruses
	• Understand strategies for preventing computer virus infections
	2. Implement computer virus detection and protection technology
	
	• Select and implement computer virus detection methods including:
	    o Install and keep up-to-date the latest anti-virus and repair software, as well as the latest computer virus identifiers
	    o Review all records of routers and firewalls
	    o Configure an intrusion prevention system to identify activities associated with computer virus infection
	• Select and implement computer virus protection techniques including:
	    o Install patches to correct bugs in the computer operating system and software
	    o Install anti-virus software and firewall products and regularly update them
	    o Avoid opening unknown links, files and applications, and perform automatic file decompression
	    o Implement anti-virus technology, real-time monitoring technology, and full platform anti-virus technology
	3. Demonstrate professional skills and attitude
	
	• Regularly review computer virus detection and protection technologies to ensure that those used are in the company's best interests
	• Ensure that the computer virus detection and protection strategy developed complies with Hong Kong's legal requirements

Assessment Criteria	The integrated outcome requirement(s) of this unit of competency is/are: • Select and use appropriate computer virus detection and protection technologies, and develop operational procedures for daily defence and system updates; and • Regularly review and formulate contingency measures to prepare for the immediate response to and recovery of system operations in the event of an emergency, thereby minimising the impact on the company's operations
Remark	