Specification of Competency Standards for ICT Operation and Support

Unit of Competency

Functional Area: Security Support

Title	Strengthen workstation protection
Code	107891L3
Range	This unit of competency applies to support personnel who are responsible for securing client workstation. Workstations are vulnerable to local and external threats, they need to be protected from as much as these threats as possible. Most organisation will have different protection procedures which support personnel need to setup before allowing user to access the workstation. This UoC illustrates some of the protection tasks and it is by no means exhaustive.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for strengthening workstation protection • Possess system troubleshooting skills • Possess detailed knowledge of security features and functions of the organisation’s operating systems • Possess good knowledge of system security concepts • Possess good knowledge of computer hardware and system software • Possess knowledge of the organisation’s security procedures and guidelines

Unit of Competency

Functional Area: Security Support

Competency	2. Strengthen workstation protection • Comprehend the organisation’s guideline for workstations protection to configure the user’s workstation. Systematically setup and configure protection features on the workstation • Setup physical security protection, including but not limited to the following: • Lock the CPU unit to prevent opening of the case • Affix a chain lock (Kensington lock) to secure position for notebooks • Setup password protection (hardware-level) for access to machine’s BIOS • Eliminate or disable unnecessary services. For example: remote access, Internet sharing, etc. • Remove unnecessary executables and registry entries to prevent attacker invoking disabled programs • Set user account to • “non-administrator” account, to prevent uncontrolled change of system settings • Avoid multi-user sharing same machine, if possible • Set system account policies • Minimum length of account password • Force change password • Set re-used policy • Setup screen save to turn off screen and power off system after a predefined period of no user activities • For systems holding confidential information, setup file encryption and access permission • Install and setup anti-virus, anti-spyware and anti-malware scanning and handling, such as: • Auto and scheduled update of virus definitions • Scheduled daily scan • Real time protection • Anti-virus application which starts on system boot • When virus or malware found, clean first (high risk) and quarantine second • Setup firewall protections • Setup auto and scheduled system updates • Create a backup image of the workstation before allowing user to use the machine • Document the system settings and configurations for internal record 3. Exhibit professionalism • Exhibit security ethics and balance the need of users with the organisation security needs when setting and configuring security protection of user’s workstations
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Comprehend the organisation’s workstation protection guidelines and able to configure and setup required security protections • Complete documents of the security settings and configuration in accordance with the organisation’s procedures
Remark	