資訊科技及通訊業《能力標準說明》能力單元

「資訊保安支援」職能範疇

名稱	加強工作站保護
編號	107891L3
應用範圍	這個能力單元適用於負責保護客戶端工作站的支援人員。工作站很容易遭受本地和外部的威脅，支援人員需要盡可能保護工作站免受這些威脅影響。大多數機構都有不同的保護措施，支援人員需要先做好有關設定，才可讓用戶存取工作站。這個能力單元列舉了部分保護工作，但並不是詳盡無遺的。
級別	3
學分	3
能力	表現要求 1. 加強工作站保護的所需知識 • 擁有排除系統故障的技能 • 熟悉機構的操作系統的安全特性及功能 • 擁有系統保安概念的良好知識 • 擁有電腦硬件及系統軟件的良好知識 • 了解機構的保安程序及指引 2. 加強工作站保護 • 了解機構的工作站保護指引，並按照指引設定用戶的工作站。有系統地設置並設定工作站上的保護功能 • 設置實體安全保護，包括但不限於以下各項： o 鎖上中央處理器組件以防機箱打開 o 扣上電腦鋼纜鎖（如肯辛頓鎖（Kensington lock）），固定筆記簿型電腦於所在位置 • 為電腦的基本輸入輸出系統（BIOS）設定密碼保護（硬件級別） • 移除或停用不必要的服務，例如：遠程存取及互聯網共享 • 刪除不必要的可執行檔案及登錄檔項目，防止攻擊者借助停用的程式發動攻擊 • 設定用戶帳號 o 設定為「非管理員」帳號，防止系統設定在沒有受到控制的情況下遭更改 o 如有可能，避免多人共用一台電腦 • 設定系統帳號政策 o 帳號密碼的最短長度 o 強制要求更改密碼 o 設定重用密碼規則 • 設定屏幕保護程式，在預定的時間內用戶沒有活動時就關閉屏幕，並熄掉系統電源 • 在保存機密資訊的系統上設定檔案加密及存取權限 • 安裝並設定病毒、間諜程式及惡意程式的掃描及處理，例如： o 自動定期更新病毒定義 o 排程每日進行掃描 o 實時保護 o 系統啟動時啟動防病毒應用程式

「資訊保安支援」職能範疇

	○ 發現病毒或惡意程式時，先清理（高風險），後隔離 • 設置防火牆保護 • 設置自動及定期的系統更新 • 讓用戶使用電腦前，建立工作站的備份映像 • 記錄系統設定及配置以作內部紀錄 3. 展示專業能力 • 在設置及設定用戶工作站的安全保護時，展示保安倫理，並平衡用戶的需要與機構的保安需要
評核指引	此能力單元的綜合成效要求為： • 了解機構的工作站保護指引，並能設置及設定所需的安全保護 • 根據機構的程序完成保安設定及配置的文件
備註	