

零售業 《能力標準說明》 能力單元

「交易安全技術」職能範疇

名稱	掌握電腦病毒檢測與防範技術
編號	107235L4
應用範圍	應用電腦病毒防範技術以建立一套完善的電腦病毒防範應對策略，當電腦病毒危機事件發生時，可以發現危機的根本原因，降低危機破壞性，保護企業的電子商務系統。
級別	4
學分	6 (僅供參考)
能力	<p>表現要求</p> <ol style="list-style-type: none"> 1. 掌握電腦病毒的基本概念和知識 <ul style="list-style-type: none"> ● 瞭解電腦病毒的基本操作原理 <ul style="list-style-type: none"> ● 瞭解電腦病毒的結構 ● 認識電腦病毒感染策略 ● 明白電腦病毒的作用機制 ● 識別電腦病毒的分類，包括： <ul style="list-style-type: none"> ● 按照病毒攻擊的系統分類，如攻擊Windows、UNIX或其他系統 ● 按照病毒的攻擊機型分類，如攻擊微型電腦、小型機或工作站 ● 按照病毒的鏈結方式分類，如源碼型病毒、嵌入型病毒、外殼型病毒、作業系統型病毒等 ● 按照病毒的破壞情況分類，如良性電腦病毒、惡性電腦病毒等 ● 按照病毒的寄生方式分類，如引導型病毒、檔型病毒、複合型病毒等 ● 按照病毒的傳播媒介分類，如單機病毒、網絡病毒等 2. 運用掌握電腦病毒檢測與防範技術 <ul style="list-style-type: none"> ● 選擇和應用系統檢測方法，包括： <ul style="list-style-type: none"> ● 使用最新病毒識別碼以及更新過的抗電腦病毒偵測與修復引擎 ● 複查所有路由器與防火牆的記錄 ● 配置IPS或IDS以辨認與感染相關的活動 ● 執行封包追蹤(packet sniffing)，以尋找符合惡意程式碼特徵的網絡通訊 ● 選擇和應用電腦病毒防範技術，包括： <ul style="list-style-type: none"> ● 修補作業系統以及其捆綁軟體的漏洞 ● 安裝並及時更新防毒軟體與防火牆產品 ● 不要點來路不明連線以及執行不明程式 ● 執行反病毒技術 ● 執行即時監視技術 ● 執行自動解壓縮技術 ● 執行全平台反病毒技術 3. 展示專業能力 <ul style="list-style-type: none"> ● 確保引入最適合的電腦病毒防範技術及應對策略，符合企業的利益 ● 確保所制定的電腦病毒防範策略不可抵觸香港法例相關的規定
評核指引	<p>此能力單元的綜合成效要求為：</p> <ul style="list-style-type: none"> ● 能夠瞭解電腦病毒的基本概念 ● 能夠識別電腦病毒分類 ● 能夠正確地選擇和應用適當的反電腦病毒技術
備註	