資訊科技及通訊業標準說明

能力單元

1. 名稱	調查資訊保安事件
2. 編號	ITSWIS517A
3. 應用範圍	爲機構調查資訊科技及通訊業保安事件，並提出可用作控告的證據 [資訊保安 - 鑑識]
4. 級別	5
5. 學分	5
6. 能力	表現要求 6.1 瞭解鑑識概念和調查技術 有能力 ▪ 瞭解資訊科技及通訊業保安問題 ▪ 瞭解調查保安事件的程序 ▪ 瞭解各種證據收集的技巧 ▪ 應用鑑識原則來評估環境 ▪ 瞭解調查計劃的框架 6.2 確定需要調查的事件 有能力 ▪ 訂定一套確定事件的指引 ▪ 確保在調查期間採取的步驟是合法的 ▪ 評估事件是否適合進行調查 6.3 制定調查計劃 有能力 ▪ 爲處理某宗調查，訂定程序 ▪ 訂定資訊收集的技術 ▪ 確定政策、程序、過程和工具的類型 ▪ 委任擁有處理調查知識的職員 ▪ 訂定記錄所有鑑識活動的框架 6.4 細查收集到的資料 有能力 ▪ 委任職員進行鑑識分析 ▪ 瞭解和詮釋已收集的資料和準備民事訴訟的證據 ▪ 從收集到的資料，整理有用的資訊和可呈堂的證據 ▪ 辨識可能觸犯法律的重要元素

	6.5 以專業的方式調查保安事件	有能力按照機構內部指引及任何適用的(本土及國際)法律與監管要求，調查保安事件
7. 評核指引	上述能力單元之綜合能力要求爲 (i) 制定一套確定保安事件的指引；並且 (ii) 制定調查資訊科技及通訊業保安事件的計劃。	
備註		