

資訊科技及通訊業 《能力標準說明》 能力單元

「內容保安」職能範疇

名稱	維護內容安全
編號	108066L3
應用範圍	本能力單元適用於所有負責推行策略的數碼媒體科技從業員。對大部份公司而言，內容保安關乎權利和知識產權 (IP) 保護。這是對的，但除了數碼版權管理 (DRM) 外，還有很多其他安全方面的細節需要考慮，並需經過驗證以保證內容安全。內容保安是資訊安全的一部份，因此本能力單元不會區分「純內容」或「純資訊」安全；但僅涵蓋與保護公司數碼媒體內容相關的安全要素。
級別	3
學分	3
能力	<p>表現要求</p> <p>1. 維護內容安全的知識</p> <ul style="list-style-type: none"> ● 具備良好的項目管理和技術性寫作的的能力 ● 深入了解計劃和推行內容保安的知識 ● 了解不同類型的內容保安和資訊保安技術 ● 了解推行內容保安的方法 ● 了解網絡和基建安全知識 ● 了解香港的內容保安和知識產權法律 ● 了解公司的安全策略 <p>2. 維護內容安全</p> <ul style="list-style-type: none"> ● 評估公司目前的內容保護計劃/設計，並決定存在或可能存在安全風險的地方，包括但不限於以下各項： <ul style="list-style-type: none"> ○ 防火牆保護規則 ○ 實體存儲系統 (伺服器、存儲區域網路 (SAN) 等) ○ 網絡安全，包括虛擬私人網絡 (VPN)，傳輸層安全性協定等 ○ 網絡攻擊保護 ● 在網站和網絡應用程式上，檢查用戶的憑證/身份認證和註冊系統，以確保所需的身份驗證元素都按照保安策略的規定正確執行。元素的例子包括： <ul style="list-style-type: none"> ○ 用戶名稱、密碼 ○ 個人身份資料 ○ 保安問題的答案/挑戰 ○ CAPTCHA 驗證碼 (全自動區分電腦和人類的公開圖靈測試) ○ 輸入結構化查詢語言 (SQL) 不能損害伺服器腳本語言 ● 檢查製作時應用的內容保護機制，例如： <ul style="list-style-type: none"> ○ 水印 ○ 加密 ○ 已設置權利/地理位置訪問權限 ● 在儲存內容到雲端時，檢視公司的混合雲安全性，並確保以下各項： <ul style="list-style-type: none"> ○ 保存在流動設備上的敏感內容/文檔已加密 ○ 儲存在雲的內容已加密 ○ 跨網絡傳輸的內容已加密。例如：傳遞系統

資訊科技及通訊業 《能力標準說明》 能力單元

「內容保安」職能範疇

	<ul style="list-style-type: none">檢視數碼版權管理 / 數碼資產管理 (DAM) 系統、證書系統、傳遞系統，以確保它們的配置正確，且所有內容均經過加密處理，並傳遞給正確的持分者 (用戶、客戶、工作人員等)檢視備份、恢復機制和程序;確保到位並且安裝妥當。員工接受足夠的演練，為緊急情況做好準備檢視安全監控，確保它可以提示/突出顯示安全異常。例如：網頁檢查安全升級、處理情況和其他內容保安程序，以確定它們是否最新且有效記錄發現和可能可以加強的領域。如有必要，告知管理層，及安排將來再次檢視。 <p>3. 展示專業精神</p> <ul style="list-style-type: none">應用行業最佳實踐經驗以保護公司儲存在內部或雲端的數碼內容。最佳實踐經驗示例：ISO 27000 標準系列
評核指引	此能力單元的綜合成效要求為： <ul style="list-style-type: none">識別和檢查保護數碼內容的安全組件檢查內容保安性，確保有系統、有方法地以分層或洋蔥式處理全面檢查所有公司的內容是否安全，並就任何需要改善的安全風險提交完整報告
備註	