

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	建立內容保安慣常做法和程序
編號	108067L3
應用範圍	本能力單元適用於所有參與實施內容保安的數碼媒體科技從業員。內容可以通過多種方式取得/創建，並通過多種途徑發佈。內容可以被機動地調整用途，並針對個人消費者/用戶度身定造。良好的內容管理慣常做法可以平衡存取和風險，以確保數碼內容受控制和保護。
級別	3
學分	3
能力	<p>表現要求</p> <p>1. 建立內容保安慣常做法和程序的知識</p> <ul style="list-style-type: none"> • 具備良好的項目管理和技術性寫作的能力 • 深入了解建立安全和操作程序的知識 • 深入了解不同類型的內容保護系統，例如： <ul style="list-style-type: none"> ○ DRM (數碼版權管理) ○ DAM (數碼資產管理) ○ 加密媒體延伸 ○ 內容分發系統 • 了解內容管理的方法 • 了解香港的內容保安和知識產權 (IP) 法律 • 了解公司對記錄文檔的標準 <p>2. 建立內容保安慣常做法和程序</p> <ul style="list-style-type: none"> • 理解公司對內容保護和安全的策略，以形成不同類形的內容保護建圖 • 檢查目前在公司中運作的內容保護系統和技術，包括但不限於以下各項： <ul style="list-style-type: none"> ○ 數碼版權管理和數碼資產管理系統 ○ SSL (安全套接層)，SHA (安全雜湊算法) 和 TLS (傳輸層安全性協定) ○ 水印 ○ 通過 HTTP 進行動態自適應流 (DASH) • 定義程序和目標受眾的範圍/目標，例如： <ul style="list-style-type: none"> ○ 定義存取控制 ○ 定義基本的加密保護 ○ 配置內容保安全管理系統 ○ 處理侵權行為 • 為程序定義操作行動，例如： <ul style="list-style-type: none"> ○ 定義視頻訪問控制 <ul style="list-style-type: none"> ▪ 允許透過某些用家生成的令牌(token)查看 ▪ 接受來自特定地域的令牌(token) ▪ 即使使用有效的令牌(token)，拒絕匿名 IP 地址訪問 • 定義註冊和登記的要求、安全系統的設置和配置，例如： <ul style="list-style-type: none"> ○ 用戶 ID - 最小的長度 ○ 密碼 - 最小的長度，驗證字符

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">○ 雙重驗證 - 使用 CAPTCHA 驗證碼檢查 (全自動區分電腦和人類的公開圖靈測試)○ 電子郵件地址 - 確認註冊● 定義當安全系統顯示非法內容訪問，或檢測到侵權/安全漏洞時所要採取的措施。另外，按角色和責任定義向上級通報的架構● 在公司簡報會中，向持分者介紹和測試程序，並獲取意見以改善程序 <p>3. 展示專業精神</p> <ul style="list-style-type: none">● 致力制定程序，在不會因錯誤傳達而造成誤解下，正確地向參閱者提供精確的指引
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">● 制定水平正確的程序，以便向持分者提供準確簡潔的細節，及保護公司內容所需的行動● 制定反映程序範圍和實現目標的程序● 制定符合公司記錄文件的標準和格式之程序
備註	