iCAP 職能發展應用平台>職能資源專區>職能單元資源查詢

職能單元代碼	INM5R1455v2
職能單元名稱	執行網路安全加密技術
領域類別	資訊科技 / 網路規劃與建置管理
職能單元級別	5
工作任務與行為指標	一、決定加密方法 1. 分析企業資料安全需求。 2. 建立新的或審核現有安全計畫，以決定加密【註1】方法。 3. 檢視各種加密技術【註2】並排定最適當的選項。 4. 評估考量各種加密選項的成本。 5. 以文件記錄加密選項與成本，並交由適當人員決定加密方法。 二、執行加密 1. 應用加密技術於企業系統。 2. 分析加密技術對使用者角色與責任的影響。 3. 告知使用者新的加密技術以及對其責任影響。 三、監控加密 1. 分析加密技術的執行結果，並確認功能與績效。 2. 檢視有關執行問題的服務台紀錄，並採取適當措施。 3. 檢討加密問題與失效部分的系統紀錄。 4. 以文件記錄加密與失效問題，並回報適當人員。
職能內涵 (K=knowledge 知識)	一、憑證相關基礎建設 二、不對稱與對稱金鑰演算法的專業知識 三、加密強度與加密種類與知識 四、單向訊息摘要知識 五、公開金鑰基礎建設（PKI）、良好隱私密碼法（PGP）與 GNU 隱私守衛（GnuPG）知識 六、安全威脅來源概念【註3】 七、傳輸控制協定或網際網路協定（TCP / IP）協定與應用知識 八、組織可能產生的安全問題與挑戰 九、無線加密協議（WEP）、wi-fi 保護存取（WPA）及 wi-fi 保護存取（WPA2）知識

職能內涵 (S=skills 技能)	一、溝通協調能力 二、企業資料安全需求分析能力 三、加密選項與成本技術文件的解讀能力 四、規劃網路安全加密執行專案 五、解決、清除與修正連線及安全問題解決能力 六、加密選項、資料安全威脅及與反制措施的研究能力 七、網路安全加密系統監控技術能力 八、網路安全加密系統功能測試能力 九、網路安全風險評估能力 十、撰寫網路安全加密紀錄與呈報實務
評量設計參考	一、評量證據 1. 分析企業的資料安全需求。 2. 建立新的或檢討現有安全計畫，以決定加密方法。 3. 排序並記錄適當的加密方法。 4. 執行加密方法並告知使用者影響效應。 5. 監控與記錄加密的問題，並通知適當人員。 二、評量情境與資源 1. 可進行加密安裝的場地。 2. 評量項目如：運作網路、伺服器、加密軟體、加密工具。 3. 視情況與其他單位進行工作場域與工作職責方面的全面性評量。 4. 評量流程與技巧須因地、因人制宜。 5. 必要時提供適當的學習和評量協助。 6. 提供特殊需求人士使用的所需設備與支援。 三、評量方法 1. 採用多種評量方式來評量實務技能與知識。 2. 評量受評者檢討說明企業安全要求與安全計畫的分析與規劃報告，包括面臨的挑戰與解決方法。 3. 評估受評者提出最適當加密系統的證明文件。 4. 口頭或書面提問，評量受評者有關加密種類及演算法功能與特性的知識。 5. 觀察受評者執行與監控加密系統所需的任務。

	6. 若採實習評量，宜結合目標提問方式進行評量所需知識。
說明與補充事項	【註1】加密：包含不對稱公開金鑰密碼、數位簽名、PGP、PKI、PKZIP、RSA 加密法、SSH、安全資料傳輸層（SSL）等。 【註2】加密技術：包含 Blowfish 先進 CS、Cryptainer LE、GnuPG、內建作業系統檔案加密系統、開放 VPN、PGP 等。 【註3】安全威脅來源概念：如竊聽、資料攔截、資料惡化、重播安全、資料造假與驗證問題等。

更新紀錄
2021 年修訂職能內容。