

課程名稱：18442_中小企業資安教育訓練影片 課程摘要

本摘要由 Gemini AI 協助生成，僅供參考

1. 適合對象與能力門檻

- **適合族群：**初學者、中階主管、老闆、特定職種（如中小微型企業同仁、非營利組織/NGO 人員、資訊與資安管理人員、委外專案管理人員）。本課程專為希望建立基本資安認知、提升個人與組織防護力，或需負責內部資安宣導與委外廠商管理的人員設計。
- **能力門檻：**入門。無須具備高深的資安或程式開發背景，課程著重於觀念建立、日常防護習慣與實務管理技巧。

2. 課程核心大綱與架構圖

- **章節架構：**
 - **章節一：基本資安防護實務** — 認識資安威脅趨勢（Cyber Kill Chain、社交工程、勒索軟體）、資通安全三大目標（CIA）與業務不中斷概念。
 - **章節二：常見資安風險與實務防護** — 涵蓋資料安全（3-2-1 備份原則、隨身碟加密）、社交工程防範、行動裝置安全、通訊軟體/社群帳號防護、實體安全與人力資源安全。
 - **章節三：網路安全管理實務** — 介紹防火牆（Deny-All 規則）、網路區隔、IoT/物聯網裝置安全（如修改預設密碼、印表機與攝影機防護）、無線網路安全（WPA2/WPA3、隱藏 SSID）、多因素驗證（MFA）與電子郵件安全。
 - **章節四：資安管理基礎實務與個資法** — 介紹資訊安全管理系統（ISMS / ISO 27001）與 PDCA 迴圈、資產盤點與風險評估、存取控制、備份與營運持續計畫；並深入解析《個資法》生命週期（蒐集、處理、利用、銷毀）、特定目的告知、安全維護計畫與外洩通報（72 小時內）。
 - **章節五：委外資安管理實務** — 剖析系統委外生命週期（計畫、選商、履約、驗收、維運）、服務等級協議（SLA：如 RTO、RPO、MTPD 量化指標）、安全程式開發（SSDLC、原碼掃描、弱

點掃描、滲透測試）與個資委外監督及民事/行政責任。

3. 必備前置知識清單

- **基本電腦與行動裝置操作**：具備網頁瀏覽、收發電子郵件、使用雲端服務與手機 APP 的基本能力。
- **無特殊技術背景要求**：無須具備路由器設定或攻防等高階技術基礎，課程以管理觀念與實務溝通為主。

4. 專有名詞與概念辭典

- **資安三要素 (CIA Triad)**：
 - **機密性 (Confidentiality)**：確保僅有獲得授權的人員才能存取資料。
 - **完整性 (Integrity)**：確保資料與系統正確無誤，未經授權不得被篡改。
 - **可用性 (Availability)**：確保經授權的使用者在需要時，系統與資料皆可正常提供服務。
- **3-2-1 備份原則**：資料至少保持 **3** 份副本，儲存於 **2** 種不同的媒介，且至少有 **1** 份存放在異地（或雲端）。
- **社交工程 (Social Engineering)**：利用人性的弱點（如恐懼、好奇、貪心或信任）進行欺騙，誘使目標交出密碼、點擊釣魚連結或安裝惡意程式的攻擊手法。
- **Deny-All (拒絕全部)**：防火牆的最佳實踐原則，除了明確允許（Permit/Allow）通過的流量之外，其餘所有連線一律阻擋。
- **SSDLC (安全資通系統發展生命週期)**：在軟體開發的各階段（需求、設計、開發、測試、部署維運）皆注入資安考量，如進行原碼掃描與滲透測試。
- **SLA 指標 (RTO / RPO / MTPD)**：
 - **RPO (資料復原點目標)**：系統中斷時，組織所能忍受的最大資料遺失量/時間。

- **RTO (系統復原時間目標)**：系統中斷後，切換或復原至備用/基本服務狀態所允許的時間。
- **MTPD (最大可容忍中斷時間)**：系統從服務中斷到完全恢復至正常營運狀態的最大極限時間。

5. 課程學習職能對照

- **對應職能名稱**：資安管理專員/主管、個人資料保護專員、資訊委外專案經理、系統營運管理人員。
- **主要工作任務/能力指標**：
 - **[分析與決策能力]**：能進行組織資訊資產盤點與風險評估，規劃 PDCA 資安管理迴圈，訂定符合《個資法》規範的安全維護計畫與委外 SLA（量化合約指標）。
 - **[工具操作與執行能力]**：能落實 3-2-1 備份與加密機制、設定多因素驗證（MFA）、督導防火牆與網路區隔設定、執行個資盤點表編製，以及管理 SSDLC（原碼與弱點掃描）開發流程。