從盤點到防護——個資風險分析與管理實務

國立臺北商業大學 資訊與網路中心 徐國鈞 主任

目錄

01 個資盤點實務

- 個人資料定義
- 個資保護法源依據
- PDCA
- 個資法罰則及個資外洩案例
- 個人資料檔案清冊

02 風險評估操作

- 個人資料檔案風險值
- 個人資料檔案清冊範例
- 個人資料檔案風險評估表範例

03 制定改善計畫

- 風險改善計畫表
- 風險評鑑彙整表

04 實作練習

- 辨識校園常見個資風險情境

01 個資盤點實務

- 個人資料定義
- 個資保護法源依據
- PDCA
- 個資法罰則及個資外洩案例
- 個人資料檔案清冊

01 個資盤點實務：個人資料

- 基本定義：個人資料是指**自然人**之姓名、出生年月日、國民身分證統一編號、護照號碼、婚姻、家庭、教育、職業、聯絡方式、財務情況，以及社會活動。
- 識別性：個人資料分為**直接識別**與**間接識別**，直接識別為如姓名、身份證號、照片、指紋等；間接識別為可透過比對、組合等方式，足以識別特定個人的資料。

01 個資盤點實務：個人資料

- **特種個資**：包括醫療、健康、基因、性生活、健康檢查及犯罪前科資料，受更嚴格的保護規範。
- 生物特徵：指具個人專屬性足以識別個別身分之個人生理特徵資料（如指紋、臉部特徵、虹膜、聲音、掌紋，以及靜脈等）。

01 個資盤點實務：法源依據

- 個人資料保護法
- 個人資料保護法施行細則
- 私立高級中等以下學校及幼兒園個人資料檔案安全維護計畫實施辦法

01 個資盤點實務：法源依據

個人資料保護法
第 20-1 條

1. 非公務機關保有個人資料檔案者，應辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
2. 前項個人資料檔案安全維護事項、管理機制、應採取之措施及其他相關事項之辦法，由主管機關定之。

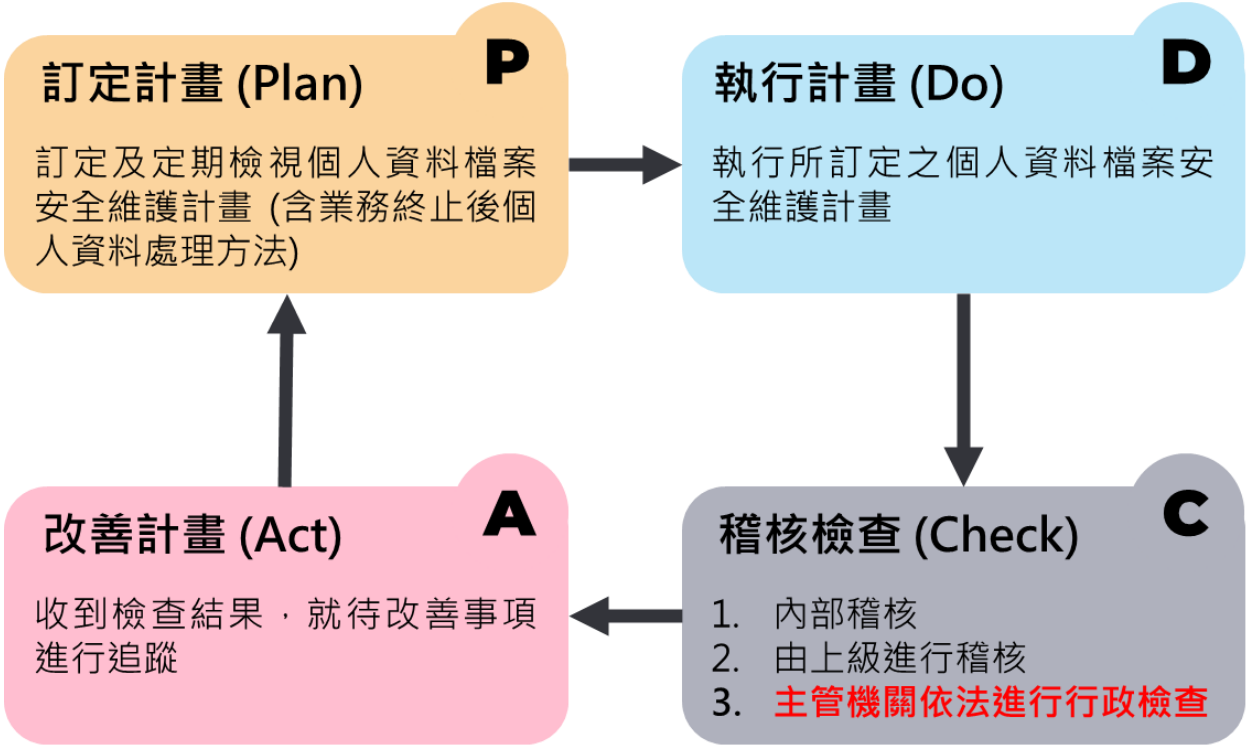
個人資料保護法施行細則
第 12 條

明確提出涵蓋個人資料檔案安全維護十一款措施之相關事項。

私立高級中等以下學校及幼兒園個人資料檔案安全維護計畫實施辦法
第 8 條

學校及幼兒園應依已界定個人資料之範圍與蒐集、處理及利用流程，分析評估可能產生之風險，訂定適當之管控措施。

01 個資盤點實務：PDCA



01 個資盤點實務：PDCA (個資法施行細則§12)

訂定計畫 (Plan)

1. 配置管理之人員及相當資源
2. 界定個人資料之範圍 (個資盤點清冊)
3. 個人資料之風險評估及管理機制 (風險評鑑表)
4. 事故之預防、通報及應變機制
5. 個人資料蒐集、處理及利用之 內部管理程序

執行計畫 (Do)

6. 資料安全管理及人員管理
7. 認知宣導及教育訓練
8. 設備安全管理

改善計畫 (Act)

11. 個人資料安全維護之整體持續改善

稽核檢查 (Check)

9. 資料安全稽核機制
10. 使用紀錄、軌跡資料及證據保存

01 個資盤點實務：個資法罰則

- 個人資料保護法第 50 條：非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。

- 2023 年立法院三讀通過個資法修正案：修正個資法第 48 條非公務機關違反安全維護義務之裁罰方式及額度，改為逕行處罰同時命改正，並提高罰鍰上限，處新臺幣 (下同) 2 萬元以上，200 萬元以下罰鍰；情節重大者，處 15 萬元以上，1,500 萬元以下罰鍰；屆期未改正者，按次處 15 萬元以上，1,500 萬元以下罰鍰。

01 個資盤點實務：個資外洩案例 (1)

案例 1：某私立科大 Excel 排序災難

承辦人員在處理學生體檢報告時，使用 Excel 進行資料排序，但操作錯誤導致姓名與報告內容錯位，結果將 A 學生的體檢報告寄給 B 學生，造成嚴重的隱私侵害。

問題根源：

- 缺乏標準作業程序 (SOP)。
- 沒有雙重檢核機制。
- 未進行抽樣檢查。
- 過度依賴單一承辦人。

01 個資盤點實務：個資外洩案例 (1)

案例 1 某私立科大 Excel 排序災難 改善方案：

- 建立標準作業程序 (SOP)：明確規範資料處理的每個步驟
- 建立雙重檢核：輸出前必須有第二人確認
- 抽樣檢查：隨機抽取 5-10 筆資料核對
- 使用郵件合併：避免手動複製貼上
- 測試寄送：先寄給自己測試格式

01 個資盤點實務：個資外洩案例 (2)

案例 2：某私立科大過度蒐集個資

學生發生意外，好心人代墊醫療費用。承辦人員為了幫忙處理退款，向代墊者索取身分證字號，涉及過度蒐集個資。

問題根源：

- 違反必要性原則，行政人員常因「以為對方需要」或「便民」而過度蒐集個資。每次蒐集個資前，都要問自己三個問題：

1. 這個個資是法律規定必須蒐集的嗎?
2. 沒有這個個資，業務就無法進行嗎?
3. 有沒有其他替代方案，可以蒐集更少的個資?

01 個資盤點實務：個資外洩案例 (2)

案例 2 某私立科大過度蒐集個資 改善方案：

錢是賠給學生的，不是賠給代墊者的。代墊者只是「先付款的人」，不需要提供個資，只需要代墊者的帳戶資訊 (用於轉帳)，不需要身分證字號。

01 個資盤點實務：個資外洩案例 (3)

案例 3：某私立大學教職員帳號被盜

教職員帳號被盜用後，駭客利用該帳號轉寄含有個資的信件給外部人員，造成大規模資料外洩。

問題根源：

- 單一驗證機制脆弱
- 密碼強度不足
- 缺乏資安警覺與應變機制

01 個資盤點實務：個資外洩案例 (3)

案例 3 某私立大學教職員帳號被盜 改善方案：

- 開啟雙重驗證 (2FA)
- 定期更換密碼
- 不使用簡單密碼
- 發現異常立即通報

01 個資盤點實務：個資盤點

- 目的：盤點**機關目前內部所存有的個人資料檔案**，並鑑別其**內容、數量、蒐集方式、處理方式、利用方式、保存期限，以及揭露方式等**資訊，以評估個資保護之風險及制定後續改善計畫，以降低風險。

01 個資盤點實務：個資盤點

- 個人資料檔案清冊應包含：**盤點單位、個人資料檔案名稱、個人資料檔案型態、特定目的、個人資料類別、有無特種個資、保有數量、蒐集的依據（法源）　、蒐集方式、處理方式、利用方式、保存期限、控制（保護）措施、銷毀方式、有無委外處理，以及對外接露**等。

01 個資盤點實務：個資盤點

- 執行頻率：**每年至少進行一次個資盤點**，期間若是遇到重大業務變動，應再次執行個資盤點。

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

個人資料檔案名稱：識別機關內部工作流程中，每一項作業所保有的個人資料，如電子郵件帳號管理系統、學籍系統等。

個人資料檔案型態：依照所保有之個資型態不同去分類，如電子檔案為電腦裡的檔案（含備份檔案）；資料庫為資訊系統中的檔案；紙本檔案等。

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

特定目的：保有個資時，蒐集、處理、利用之目的，若是超過特定目的範圍，則需重新取得同意（單一個資檔案可以有多個特定目的）。

個人資料類別：個人資料檔案中，欄位的歸類。

01 個資盤點實務：特定目的

- 教育體系常用到的特定目的：
  - 人身保險 (001)
  - 人事管理 (002)
  - 全民健康保險、勞工保險、農民保險、國民年金保險或其他社會保險 (031)
  - 存款與匯款 (036)
  - 兵役、替代役行政 (042)
  - 志工管理 (043)

法規參考：個人資料保護法之特定目的及個人資料之類別

01 個資盤點實務：特定目的

- 教育體系常用到的特定目的：
  - 非公務機關依法定義務所進行個人資料之蒐集處理及利用 (063)
  - 保健醫療服務 (064)
  - 契約、類似契約或其他法律關係事務 (069)
  - 計畫、管制考核與其他研考管理 (078)
  - 教育或訓練行政 (109)
  - 產學合作 (110)
  - 場所進出安全管理 (116)

法規參考：個人資料保護法之特定目的及個人資料之類別

01 個資盤點實務：特定目的

- 教育體系常用到的特定目的：
  - 稅務行政 (120)
  - 資 (通) 訊與資料庫管理 (136)
  - 圖書舘管理 (146)
  - 調查、統計與研究分析 (157)
  - 學生 (員) (含畢、結業生) 資料管理 (158)
  - 學術研究 (159)
  - 其他經營合於營業登記項目或組織章程等，為辦理教學、研究、行政及服務等相關事宜所需 (181)

法規參考：個人資料保護法之特定目的及個人資料之類別

01 個資盤點實務：個人資料類別

- 教育體系常用到的個人資料類別：

C001 辨識個人者：
姓名、職稱、住址、工作地址、以前地址、住家電話號碼、行動電話、即時通帳號、網路平臺申請之帳號、通訊及戶籍地址、相片、指紋、電子郵遞地址、電子簽章、憑證卡序號、憑證序號、提供網路身分認證或申辦查詢服務之紀錄及其他任何可辨識資料本人者等。

C002 辨識財務者：
金融機構帳戶之號碼與姓名、信用卡或簽帳卡之號碼、保險單號碼、個人之其他號碼或帳戶等。

法規參考：個人資料保護法之特定目的及個人資料之類別

01 個資盤點實務：個人資料類別

- 教育體系常用到的個人資料類別：

C003 政府資料中之辨識者：
身分證統一編號、統一證號、稅籍編號、保險憑證號碼、退休證之號碼、證照號碼、護照號碼等。

C011 個人描述：
年齡、性別、出生年月日、出生地、國籍、聲音等。

法規參考：個人資料保護法之特定目的及個人資料之類別

01 個資盤點實務：個人資料類別

- 教育體系常用到的個人資料類別：

C052 資格或技術：
學歷資格、專業技術、特別執照 (如飛機駕駛執照等)、政府職訓機構學習過程、國家考試、考試成績或其他訓練紀錄等。

C061 現行之受僱情形：
僱主、工作職稱、工作描述、等級、受僱日期、工時、工作地點、產業特性、受僱之條件及期間、與現行僱主有關之以前責任與經驗等。

法規參考：個人資料保護法之特定目的及個人資料之類別

01 個資盤點實務：個人資料類別

- 教育體系常用到的個人資料類別：

C081 收入、所得、資產與投資：
總收入、總所得、賺得之收入、賺得之所得、資產、儲蓄、開始日期與到期日、投資收入、投資所得、資產費用等。

C111 健康紀錄：
醫療報告、治療與診斷紀錄、檢驗結果、身心障礙種類、等級、有效期限、身心障礙手冊證號及聯絡人等。

法規參考：個人資料保護法之特定目的及個人資料之類別

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

有無特種個資：所保有之個資檔案中有無病歷、醫療、基因、性生活、健康檢查，以及犯罪前科等特種個資，如身心障礙手冊屬於醫療的一部份，為特種個資。

保有數量：清查目前所盤點之該項個人資料檔案的所有筆數，沒有銷毀的都要清查。

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

蒐集的依據（法源）：目前所盤點之個人資料檔案，是依據哪一個法規留存的，如主管機關的法規或命令、機關本身的規定等，配合個人資料告知同意書。

蒐集方式：個資的蒐集方式，如當事人直接提供或間接從其他機關取得。

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

處理方式：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。（個人資料保護法第二條第四點）

利用方式：除蒐集、處理以外的其他動作皆為利用，需在原本宣告之特定目的內。

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

保存期限：所有個人資料檔案都應依據相關法規要求，設有保存年限。如學籍資料依據高級中等學校學生學籍管理辦法，需永久保存。

銷毀方式：保存期限已屆，需定期執行銷毀作業，並留下銷毀紀錄。不同的資料類型有不同的銷毀方式，如紙本檔案使用碎紙、水銷；電子檔、資料庫使用刪除等方式。銷毀紀錄需留存五年備查。

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

控制（保護）措施：不同的資料類型有不同的控制（保護）措施，如紙本檔案使用上鎖的櫃子、有門禁管理的儲藏室等；電子檔使用加密存放；資料庫使用定期備份等措施。

委外處理：指由機關以外的單位、廠商處理，需有契約書，包含雙方之權利、義務及罰則；合約結束後資料的刪除與返還等。

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

對外揭露

：指將資料提供給機關以外的第三方，如上傳給主管機關等。

02 風險評估操作

- 個人資料檔案風險值
- 個人資料檔案清冊範例
- 個人資料檔案風險評估表範例

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

個人資料檔案價值	內容
高 (3)	含有直接或間接識別之個人資料與**特種個資**者。
中 (2)	• 含有直接或間接識別之個人資料與**財務資訊（如薪資、局帳號等）**，但不含特種個人資料者。 • 含有個人資料類別 **C003 政府資料中之辨識者（如身分證統一編號、統一證號、稅籍編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等）**者。
低 (1)	含有**姓名、員工編號、學號等**直接或間接識別個人之資料。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

  個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

衝擊程度	對當事人損害影響
高 (3)	個資檔案外洩造成當事人身心受到危害、社會地位受到損害，或衍生財物損失，當事人個人權益非常嚴重受損。
中 (2)	個資檔案外洩導致當事人隱私遭冒犯，當事人個人權益嚴重受損。
低 (1)	個資檔案外洩僅導致個人權益輕微受損。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

  個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

衝擊程度	對組織財務影響
高 (3)	個資檔案 2,000 筆以上。
中 (2)	個資檔案 30 筆以上，未滿 2,000 筆。
低 (1)	個資檔案未滿 30 筆。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

  個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

衝擊程度	對組織營運影響
高 (3)	遭禁止蒐集、處理或利用個人資料，或經命令刪除、沒入、銷毀個人資料時，對組織聲譽及**關鍵業務運作**造成影響。
中 (2)	遭禁止蒐集、處理或利用個人資料，或經命令刪除、沒入、銷毀個人資料時，對組織聲譽及**單一部門業務運作**造成影響。
低 (1)	遭禁止蒐集、處理或利用個人資料，或經命令刪除、沒入、銷毀個人資料時，對組織聲譽及**該業務流程運作**造成影響。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

  個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

可能性	作業管理規定
高 (3)	未建立相關作業管理規定及文件，亦無任何安全控管。
中 (2)	• 已建立相關作業管理規定及文件，但部分未落實安全控管。 • 未建立相關作業管理規定及文件，但已有實施部份安全控管。
低 (1)	已建立相關作業管理規定及文件，且已落實安全控管。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

  個人資料風險值 = **個人資料檔案價值** * **Max (衝擊程度)** * **Max (可能性)**

可能性	教育訓練
高 (3)	單位內人員前一年度接受教育訓練的達成率低於 60%。
中 (2)	單位內人員前一年度接受教育訓練的達成率低於 61% 至 90%。
低 (1)	單位內人員前一年度接受教育訓練的達成率 91% 以上。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

  個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

可能性	個資檔案不當存取
高 (3)	單位過去一年內曾發生一次（含）以上個資檔案不當存取事件。
中 (2)	單位過去三年內曾發生一次（含）以上個資檔案不當存取事件。
低 (1)	單位過去三年內不曾發生資檔案不當存取事件。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

  個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

可能性	個資盤點落實度
高 (3)	前一年度稽核發現： • 個資檔案未納入盤點達 9 項（含）以上。 • 未執行個資盤點作業。
中 (2)	前一年度稽核發現： • 個資檔案未納入盤點達 3-6 項。 • 已執行個資盤點作業，但內容不完整，達 6 項（含）以上。
低 (1)	前一年度稽核發現： • 個資檔案未納入盤點有 2 項（含）以下。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

  個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

可能性	個資保存
高 (3)	前一年度稽核發現： • 個資檔案未依程序保存達 7 項（含）以上。 • 單位未有可上鎖存放區域。
中 (2)	前一年度稽核發現： • 個資檔案未依程序保存達 3-6 項。 • 單位已有可上鎖存放區域，但個資檔案未置於該處。
低 (1)	前一年度稽核發現： • 個資檔案未依程序保存有 2 項（含）以下。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

  個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

可能性	個資銷毀
高 (3)	前一年度稽核發現： • 個資檔案未依程序銷毀達 7 項（含）以上。 • 未執行個資銷毀作業。
中 (2)	前一年度稽核發現： • 個資檔案未依程序銷毀有 3-6 項。 • 已執行個資銷毀作業，但未留存相關紀錄。
低 (1)	前一年度稽核發現： • 個資檔案未依程序銷毀有 2 項（含）以下。

- **個人資料檔案清冊範例（部分）**

盤點單位	個資檔案名稱	個資檔案型態	特定目的	個人資料類別	有無特種個資	保有數量（總數）	蒐集的依據（法源）	蒐集方式	處理方式
系統網路組	電子郵件帳號管理系統	資料庫	109 135 137	C001 C051 C073	無	2,250	校園網路管理辦法、通訊與作業管理程序書	直接蒐集	輸入、編輯、更正、複製、檢索、刪除、輸出、連結、紀錄、儲存、內部傳送

利用方式	保存期限	控制（保護）措施	銷毀方式	委外處理	對外揭露
聯絡、統計、分析、帳號驗證、通知	教職員離校後 5 年	資料庫保存	資料庫紀錄刪除	無	教育部社交工程演練

https://reurl.cc/zq3EAV

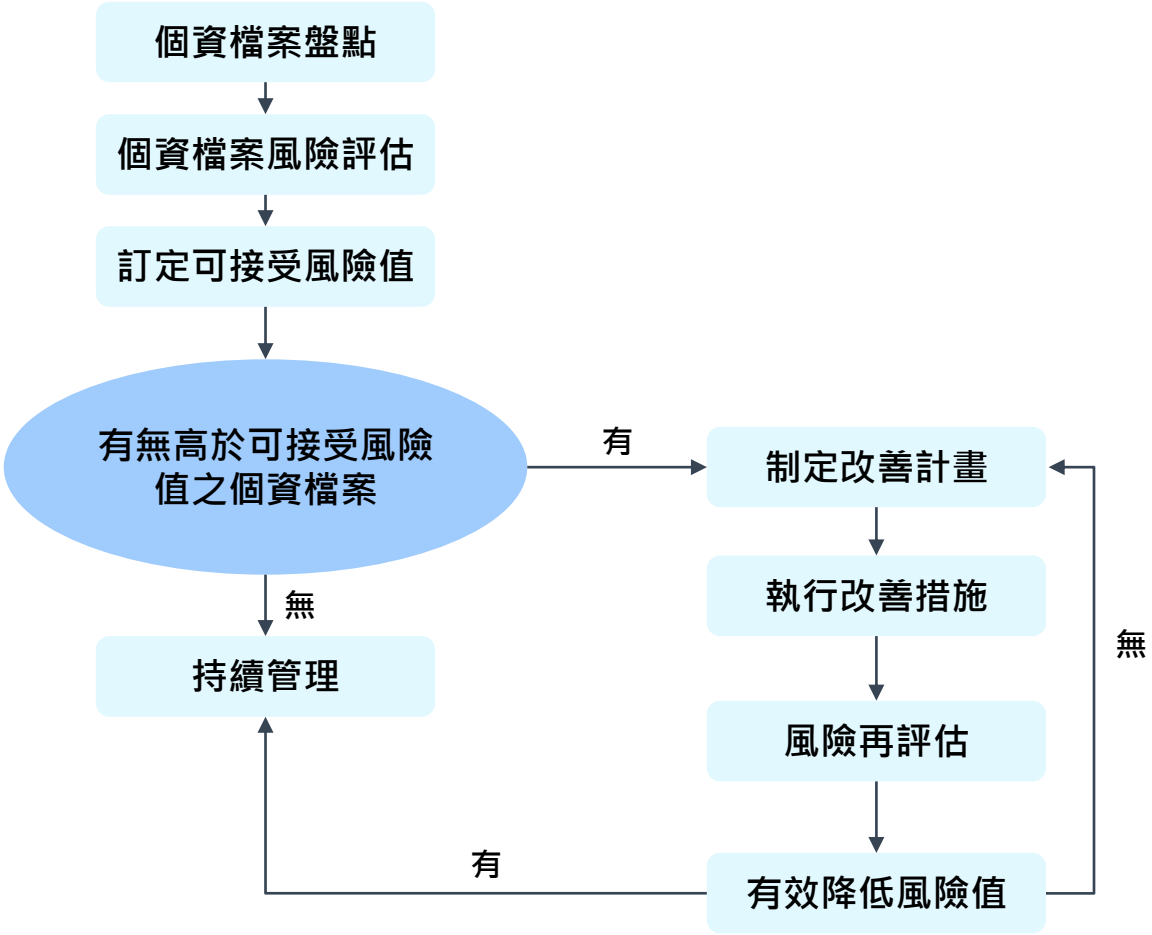
- **個人資料檔案風險評估表範例（部分）**

個資檔案名稱	個資價值 (V)	衝擊程度評估 (I)				可能性評估 (P)				風險值 (R) = V*I*P
		對當事人損害影響 (1)	對組織財務影響 (2)	對組織營運影響 (3)	評估值 Max (1,2,3)	作業管理規定 (4)	教育訓練 (5)	個資檔案不當存取 (6)	評估值 Max (4,5,6)	
電子郵件帳號管理系統	1	1	3	1	3	1	2	1	2	6

02 風險評估操作：個人資料檔案風險值

- 根據上述所估算出的個人資料風險值會落在 1-27 分之間。
- **可接受風險值**之設定，得依現有資源、管理規範及政策重點加以考量，並經會議決議後予以確定；亦可採風險值分群方式，優先處置屬高風險等級之項目。

風險等級	風險值
高	19-27
中	10-18
低	1-9


個資檔案盤點
個資檔案風險評估
訂定可接受風險值
有無高於可接受風險值之個資檔案
有
無
制定改善計畫
執行改善措施
風險再評估
有效降低風險值
無
有
持續管理

03 制定改善計畫

- 風險改善計畫表
- 風險評鑑彙整表

03 制定改善計畫：風險改善計畫表

- 制定風險改善計畫，經主管審核後實施改善措施；
- 追蹤改善成果。
- 風險改善計畫表範例（部分）：

個資檔案名稱	風險現況說明	改善建議措施	執行人員	預計完成日期	備註
電子郵件帳號管理系統	部分帳號權限設定未依人員職務即時調整，退離職人員帳號停用流程未完全落實，存在不當存取風險。	• 建立即時異動通知機制，確保人員異動時帳號權限同步更新。 • 每月進行帳號清查並紀錄。 • 制定帳號管理作業程序並加強人員教育訓練。	系統網路組承辦人	2026 年 6 月 30 日	-

03 制定改善計畫：風險評鑑彙整表

- 將大於可接受風險值或高風險等級個資檔案彙整於風險評鑑彙整表；
- 完成改善措施後，再次評估風險值是否降低。
- 風險評鑑彙整表範例（部分）：

個資檔案名稱	風險再評估									
	個資價值 (V)	衝擊程度評估 (I)				可能性評估 (P)				風險值 (R) = V*I*P
		對當事人損害影響 (1)	對組織財務影響 (2)	對組織營運影響 (3)	評估值 Max (1,2,3)	作業管理規定 (4)	教育訓練 (5)	個資檔案不當存取 (6)	評估值 Max (4,5,6)	
電子郵件帳號管理系統	1	1	1	1	1	1	1	1	1	1

04 實作練習

- 辨識校園常見個資風險情境

實作練習：辨識校園常見個資風險情境

情境 1：成績單誤寄造成個資外洩

導師在寄送段考成績單電子檔給家長時，不慎將整班的成績總表附在信件中，導致所有學生的姓名、學號、成績等資料被所有家長看到。

練習目標：

- 辨識外洩原因（作業流程疏失、未使用密件副本等）。
- 分析受影響資料類型與風險高低。
- 討論改善流程（檔案權限、寄信前檢查、分批寄信等）。

實作練習：辨識校園常見個資風險情境

情境 2：委外廠商未落實資安措施

委外廠商受託維護校內資訊系統，但工程師使用個人USB隨身碟存放學生資料，且未加密。隨身碟遺失後，可能包含學生名冊、聯絡資料及特殊身分記載。

練習目標：

- 辨識委外風險與責任分工。
- 確認風險屬性（資料未加密、設備未受控、違反契約要求）。
- 討論應加入的委外管理規範與稽核措施。

實作練習：辨識校園常見個資風險情境

情境 3：學務處公告遺失物時誤將學生資訊曝光

學務處在公布遺失物認領資訊時，將拾獲的學生證拍照放上校務系統公告欄，照片中清楚顯示學生姓名、照片、學號及班級等資料，導致不必要的個資曝露。

練習目標：

- 辨識公告資訊是否超出必要範圍。
- 判斷哪些資料屬個資、是否已涉及「目的外利用」。
- 討論公告時的匿名化方式（遮蔽學號、僅描述物品特徵等）。
- 研擬改善措施（公告流程、審核機制、人員教育訓練）。

感謝聆聽