風險評估教育訓練

德諾科技服務

DeKnow
Technology Services

簡報說明

- 個資法定要求
- 風險評估與風險處理
- 練習：風險評估
- 問題討論

進行風險評估的要求

- 個資法第 18 條

  公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

- 施行細則第 12 條 本法第六條第一項第二款所稱適當安全維護措施、第十八條所稱安全維護事項、第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。 前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則

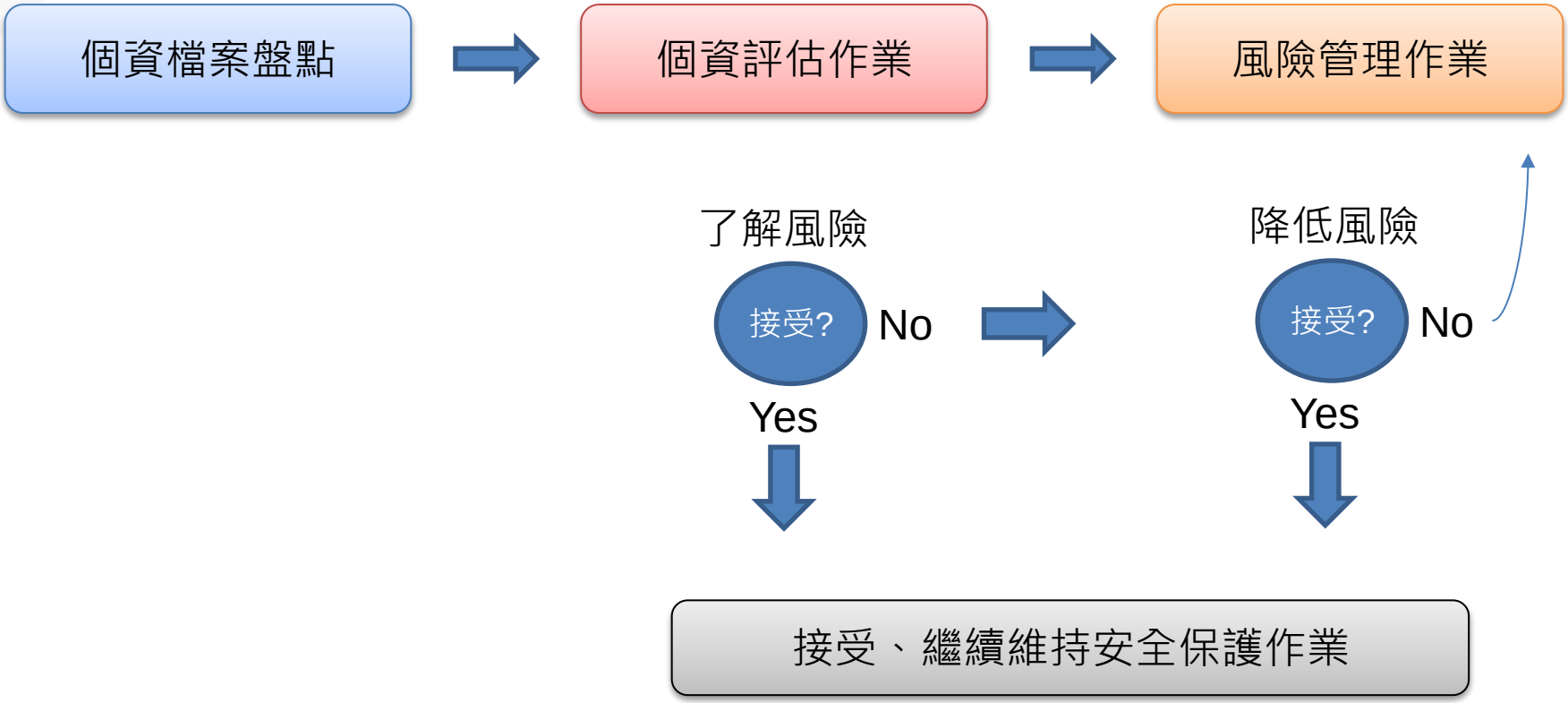
個人資料事件管理要求- 施行細則12

- 適當安全維護措施要求
  - 一、配置管理之人員及相當資源
  - 二、界定個人資料之範圍
  - 三、個人資料之風險評估及管理機制
  - 四、事故之預防、通報及應變機制
  - 五、個人資料蒐集、處理及利用之內部管理程序
  - 六、資料安全管理及人員管理
  - 七、認知宣導及教育訓練
  - 八、設備安全管理
  - 九、資料安全稽核機制
  - 十、使用紀錄、軌跡資料及證據保存
  - 十一、個人資料安全維護之整體持續改善

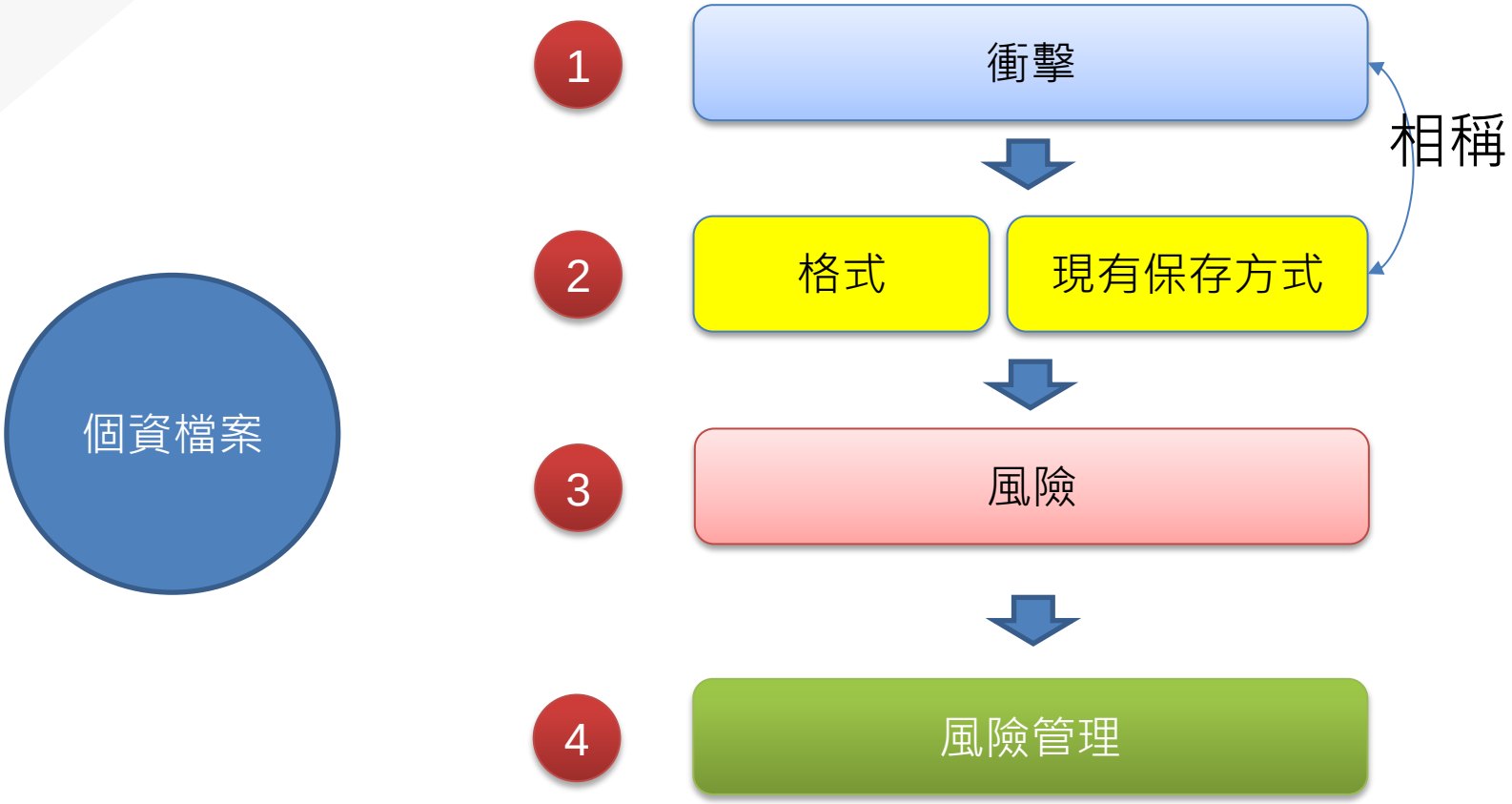
風險評估與風險處理

DeKnow
Technology Services

風險評估與風險處理


個資檔案盤點
個資評估作業
風險管理作業
了解風險
接受?
No
Yes
降低風險
接受?
No
Yes
接受、繼續維持安全保護作業

風險評估理論 → 衝擊



風險分級

- 風險分級-依數量 (表格內之數字為參考值，可調整)

分級	個人資料數量
小量	個人資料數量小於 1,000 筆
中量	個人資料數量介於 1,001筆-10,000筆
大量	個人資料數量 10,001筆以上

- 筆數的估算方式，個資法第28條，以每人每一事件新臺幣五百元以上二萬元以下計算
- 所以1,000筆大約2千萬，10,000筆就是上限2億
- 可依照遭受損害金額損失為考量點，或者是就現有握有之資料量進行資料筆數分級之調整

風險分級

- 風險分級-依蒐集資料欄位 (可依學校現況調整)

分級	個人資料欄位
低	1. 僅單一個人資料欄位
中	1. 兩種以上個人資料欄位組合(如：姓名及電話、姓名及學號) 或 2. 含身份證字號 或 護照號碼 或 3. 個人詳細學籍資料
高	1. 高風險個人資料(如財務資料、完整個人資料、敏感性的協商內容、宗教或信仰) 2. 特種個人資料(醫療、基因、性生活、健康檢查、犯罪前科)

風險分級

- 特種個人資料資訊
  - 個人資料保護法第6條，病歷、醫療、基因、健康檢查、性生活及犯罪前科等資訊。
- 高風險個人資料資訊
  - 含身份證字號或護照號碼、銀行帳號、財務資訊(不含法人帳號資訊)、個人詳細的特徵描述、可能會影響當事人權益的敏感性協商內容。
  - 完整個人資料(profile)：例如完整人事資料
- 敏感性個人資料資訊
  - 種族、政治傾向、宗教或信仰、性生活

衝擊等級

衝擊性	評估標準
低	1. 個人資料數量小於 1,000 筆 2. 僅單一個人資料欄位
中	1. 個人資料數量介於 1,001筆-10,000筆 2. 兩種以上個人資料欄位組合(如：姓名及電話、姓名及學號) 或 3. 含身份證字號 或 護照號碼 或 4. 個人詳細學籍資料
高	1. 個人資料數量 10,001筆以上 2. 高風險個人資料(如財務資料、完整個人資料、敏感性的協商內容、宗教或信仰) 3. 特種個人資料(醫療、基因、性生活、健康檢查、犯罪前科)

格式分類

- 書面/紙本格式
  - 包括一般書表、單據、手寫稿...等
- 電子文件格式
  - 包括網頁、及email 等、電子公文等被視為電子文書之書面
- 檔案格式
  - 包括各種電子檔格式、備份檔案或暫存檔、郵件附件等，與電子書面格式之不同為此類檔案主要利用方式為檔案，通常用於傳遞或保存。
- 資料庫格式
  - 存放於資料庫主機內之資料。(資料庫之備份檔案屬於檔案格式)

風險分級

風險分級-保存方式

形式 / 保存方式	書面/紙本	電子文件/檔案 (郵件、公文、Word、Excel)	資料庫
高安全保存	上鎖	已有存取控制 且 內容已使用加密技術保護	僅有系統管理者 可存取
中安全保存	1. 具基本防護遮蔽 或 2. 集中存放 或 3. 專人管理	1. 使用者皆有獨立帳號密碼 2. 具存取控制 且 加上密碼保護	獨立帳號密碼 且 已區分權限
低安全保存	未有管理	1.未有任何存取管制措施 或 2.共用帳號	1. 未有任何存取 措施 或 2. 共用帳號

風險評估等級

- 風險評估等級 (也可以換成分數進行評估)

衝擊性 / 保存方式	低	中	高
高安全保存	低風險	低風險	低風險
中安全保存	低風險	中風險	高風險
低安全保存	低風險	高風險	高風險

風險評估等級

- 風險評估等級 (換成分數評估方式)

衝擊性 / 保存方式	低 (1)	中 (3)	高 (5)
高安全保存(1)	1	3	5
中安全保存(3)	3	9	15
低安全保存(5)	5	15	25

風險評估工作底稿

			風險評估				
			衝擊等級 (低/中/高) (1/3/5)			保存方式 (低/中/高) (5/3/1)	風險評估等級
終點個資檔案 (蒐集或處理後的個資檔案)	檔案形式 如：紙本、電子檔、資料庫	存放方式/保存方式 (個資檔案存放地點、主機或保存方式) 如：契約部上鎖櫃子、商管系統資料庫.....	數量	資料欄位	衝擊等級	保存方式	
A.2.01.網路報名資料處理	**資料庫**	**招生資訊系統伺服器**		3			
				1 3 5			
考生報名表	**紙本**	**招生組承辦人**					

用下拉式選單進行各風險因子值之填寫

Q & A