個人資料保護安全管理

個人資料管理文件宣導教育訓練

課程大綱

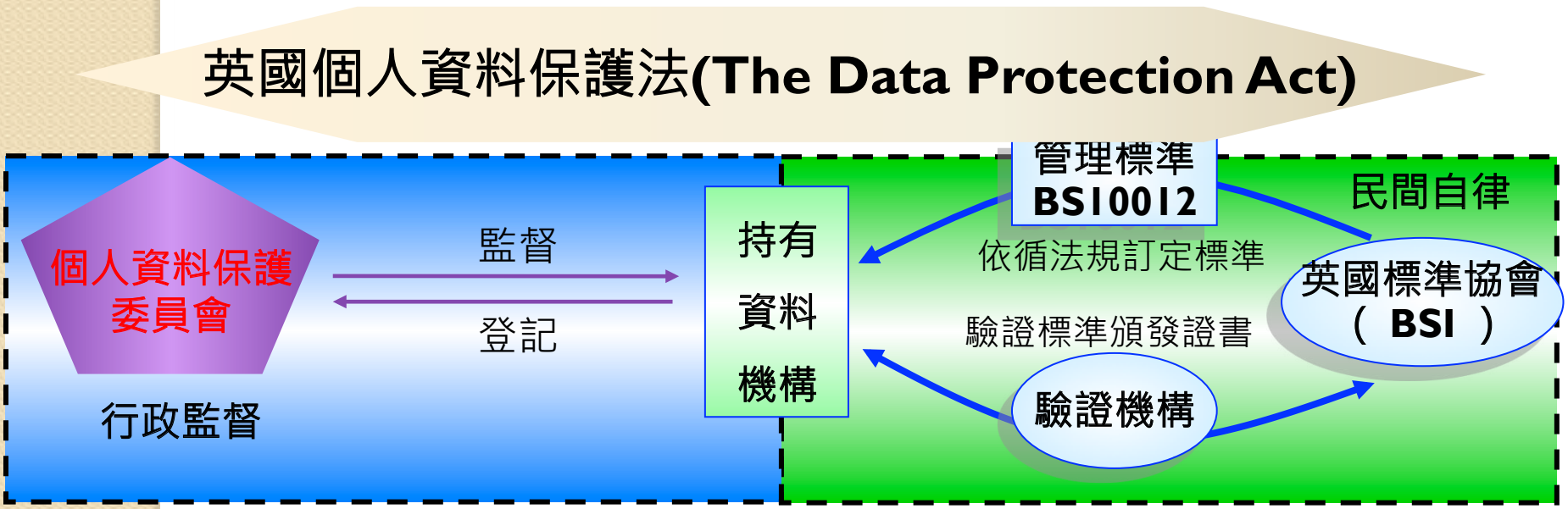
- BS 10012 標準暨個人資料保護法文件控管要求
- 個人資料管理制度文件架構暨文件生命週期
- 個資侵害事故之緊急應變
- 實作討論

課程大綱

- BS 10012 標準暨個人資料保護法文件控管要求

英國BS 10012

- 英國於1998年將歐盟之「個人資料保護指令」與「電子通訊隱私指令」內國法化為「個人資料保護法」（The Data Protection Act 1998）。並由**個資保護委員**（Information commissioner ）監督法令執行。
- 2001、2007修正擴大個人資料**適用範圍**，引發適用困擾。
- 英國標準協會（BSI）於2009年5月順應企業需要正式推出一套個人資料管理之標準（BS 10012 ），協助企業遵循英國個人資料保護法。

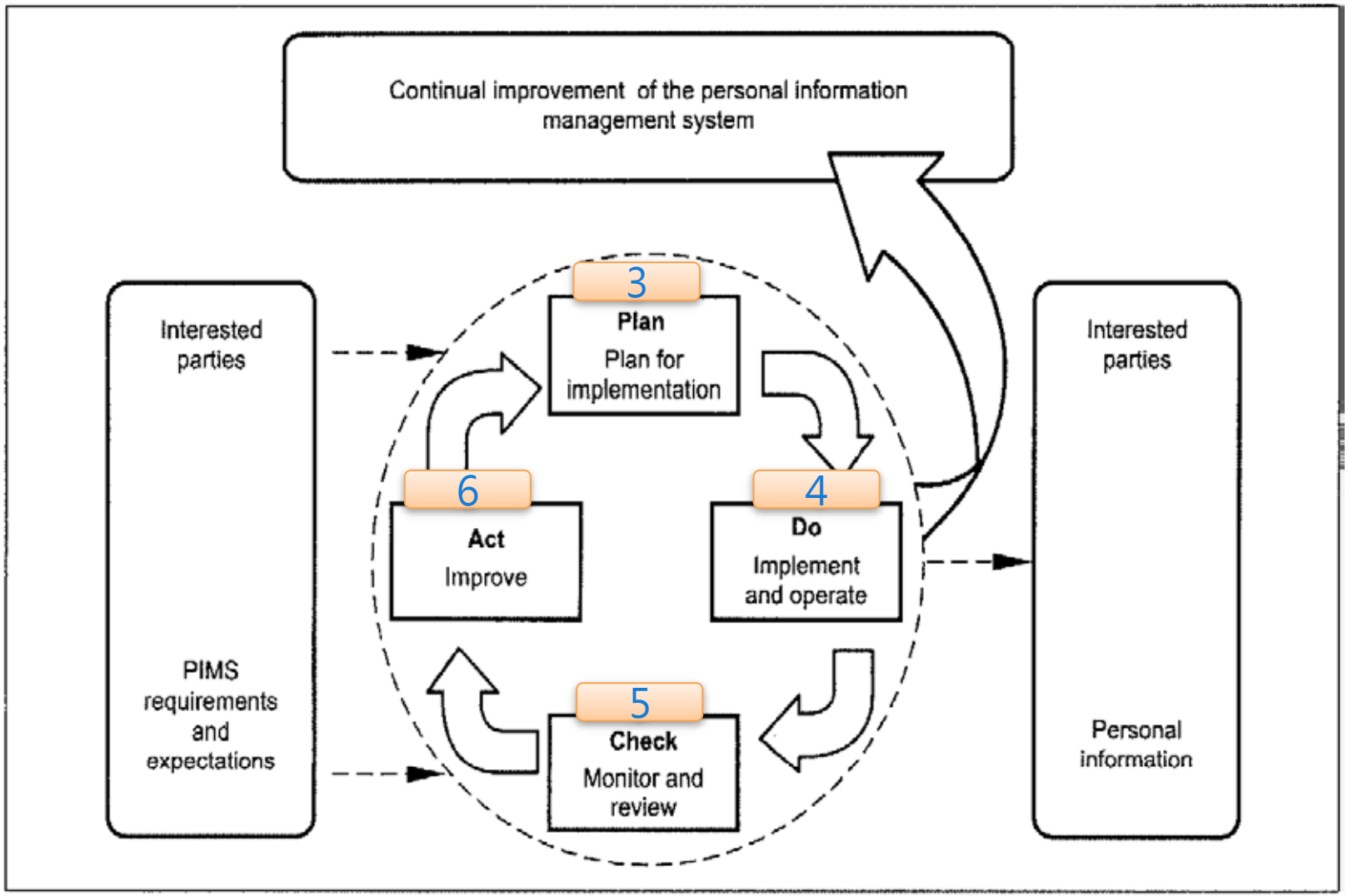


資料參考來源：經濟部

BS 10012 個人資料管理系統

- BS 10012的全名為「資料保護–個人資訊管理系統之要求（Data protection–Specification for a personal information management system）」，其中，資料保護法案所要求應遵守的8項資料保護原則，非常適合各組織作為制定個人資料保護的參考，內容說明如下：
- 個人資料不可以非法或不公正方式蒐集、處理。
- 個人資料應限於以特定目的之方式蒐集、處理。
- 個人資料應以充分、相關，而非逾越其原本之目的處理。
- 個人資料應求準確，並在必要時及時更新。
- 個人資料之保存，不得超過其原定目的之保存期限。
- 個人資料之處理，應依照當事人之權限及法令規範。
- 組織應採取適當的資料保護技術和措施，防止個人資料遺失或毀壞。
- 個人資料不得轉移到歐洲經濟區以外的國家或地區。

Plan-Do-Check-Act (PDCA)循環



規劃個人資料管理系統PIMS-1

- 3.1 建立和管理 PIMS
- 3.2 PIMS 的範圍和目標
- 3.3 個人資料管理政策
- 3.4 政策內容
- 3.5 職責和歸責性
- 3.6 資源提供
- 3.7 將PIMS嵌入組織文化

規劃個人資料管理系統PIMS-2

- 3.1 建立和管理 PIMS
  - 組織應建立、實作、維護及持續改進PIMS以符合3.2 ~ 3.7的要求
- 3.2 PIMS 的範圍和目標
  - a) 個人資料管理需求
  - b) 組織的目標與義務
  - c) 組織可接受的風險等級
  - d) 適用之法令、規章、契約(合約)與專業職責
  - e) 個人和其他利害關係人之利益

規劃個人資料管理系統PIMS-3

- 3.3 個人資料管理政策
  - 組織應確保高階管理階層被附與發行及維護個人資料管理政策之責，而其政策中應明訂政策框架，並展現對於遵循個人資料保護法與好的實務的支持與承諾。

NOTE *Senior management might consist of the Board of Trustees/Directors, the Chief Executive and senior workers, the partners of the organization or the owner of a sole trader company.*

規劃個人資料管理系統PIMS-4

- 3.4 政策內容
  - a) 僅於合法組織需求下，始得進行個人資料之處理
  - b) 僅針對特定目的蒐集必要的個人資料，且不過度的處理個人資料
  - c) 明確告知當事人其個人資料將如何被使用及被誰使用
  - d) 僅處理相關且適當的個人資訊
  - e) 公平與合法的處理個人資訊(參考 4.7);
  - f) 組織應維護一份個人資料清冊(參考 4.2);
  - g) 確保個人資料的正確性，並於必要時進行更新
  - h) 僅依法或合法的組織目的下保存個人資料

規劃個人資料管理系統PIMS-5

- i) 尊重當事人對其個人資料所能行使之權利，包含其申請閱覽權
- j) 確保所有個人資料安全
- k) 當組織將個人資料傳輸之非歐盟成員之國家時，應確保其具善良保護之機制
- l) 個人資料保護法令所允許之例外情形的應用
- m) 發展與建立PIMS，使個人資料保護政策能實行
- n) 鑑別內、外部利害關係者及其參與PIMS治理與運作的程度
- o) 於PIMS明確界定員工之責任和歸責性(參考3.5)

規劃個人資料管理系統PIMS-6

- 3.5 職責和歸責性

高階管理團隊應負起組織管理個人資料之責。

(可參考4.1.1).

- 職責應包含：
  - a) 核准個人資料管理政策
  - b) 依政策發展和施行PIMS
  - c) 應遵循政策執行安全及風險管理 (可參考4.13.1)
- 應指派一位或多位合適或具經驗的同仁負責日常個人資料管理政策的遵循(可參考4.1.2)
- 藉由流程與程序的實行、適當的員工發展或對於不符合事項制訂管控程序，以確保所有同仁皆能遵循個人資料管理政策之要求

規劃個人資料管理系統PIMS-7

- 3.6 資源提供
- 組織應決定並提供建立、實行、操作和維護PIMS的資源。
- 3.7 將PIMS嵌入組織文化

  a) 透過持續的教育訓練與認知課程，以提高、強化與維持所有員工對PIMS的認知

  b) 建立對PIMS認知訓練有效性評量程序

  c) 對所有員工傳達以下的重要性：
  - 1) 達成PIMS目標
  - 2) 遵循政策
  - 3) 對政策的持續改善

  d) 確保每個員工都瞭解他們如何影響組織PIMS

PIMS的建置與運作-1

- 4.1 責任的配置(Key appointments)
  - 4.1.1 高階管理階層
  - 4.1.2 遵循政策的日常職責
  - 4.1.3 資料保護代表
- 4.2 辨識及記錄個人資料的使用情況
  - 4.2.1 組織應維護一份個人資料分類清冊
  - 4.2.2 具高風險的個人資料
- 4.3 認知及教育訓練
- 4.4 風險評鑑

PIMS的建置與運作-2

- 4.5 PIMS 持續更新
- 4.6 通告
- 4.7 公正與合法的處理
  - 4.7.1 個人資料的蒐集與處理
  - 4.7.2 隱私公告與聲明之記錄
  - 4.7.3 隱私公告與聲明之取得
  - 4.7.4 隱私公告與聲明之可用性
  - 4.7.5 第三方

PIMS的建置與運作-3

- 4.8 個人資料處理的目的
  - 4.8.1 處理準則
  - 4.8.2 新目的的同意
  - 4.8.3 資料分享
  - 4.8.4 資料配對
- 4.9 適當、相關且不過度
  - 4.9.1 適當性
  - 4.9.2 相關且不過度
- 4.10 正確性

PIMS的建置與運作-4

- 4.11 保留及處置
- 4.12 個人的權利
  - 4.12.1 個人的權利(符合法定時間限制)
  - 4.12.2 抱怨與申訴
- 4.13 安全議題
  - 4.13.1 安全控制
  - 4.13.2 儲存及管理
  - 4.13.3 傳輸
  - 4.13.4 存取控制
  - 4.13.5 安全評估
  - 4.13.6 安全事故管理

PIMS的建置與運作-5

4.14 將個人資料傳輸於EEA(歐盟)之外
(EEA=European Economic Area)

- 4.15 揭露予第三方
- 4.16 轉包處理
- 4.17 維護

PIMS的監控與審查-1

- 5.1 內部稽核
  - 5.1.1 稽核計畫
  - 5.1.2 稽核員的挑選
  - 5.1.3 稽核需求
- 5.2 管理審查
  - a)來自PIMS 使用者之回饋
  - b)由組織人員所辨識及提升之風險
  - c)稽核結果
  - d)程序審查之紀錄
  - e)資訊技術提升及替換之結果

PIMS的監控與審查-2

- f)來自主管機關評估後之正式要求
- g)抱怨事件的處理
- h)已發生之資安事故及資料外洩事件

- 管理審查應提供所有可能造成PIMS變更之詳細資訊，其資料來源可為政策的調整、可能影響作業遵循之程序與技術。
- 當PIMS發生重大變更後，應立即執行稽核作業。

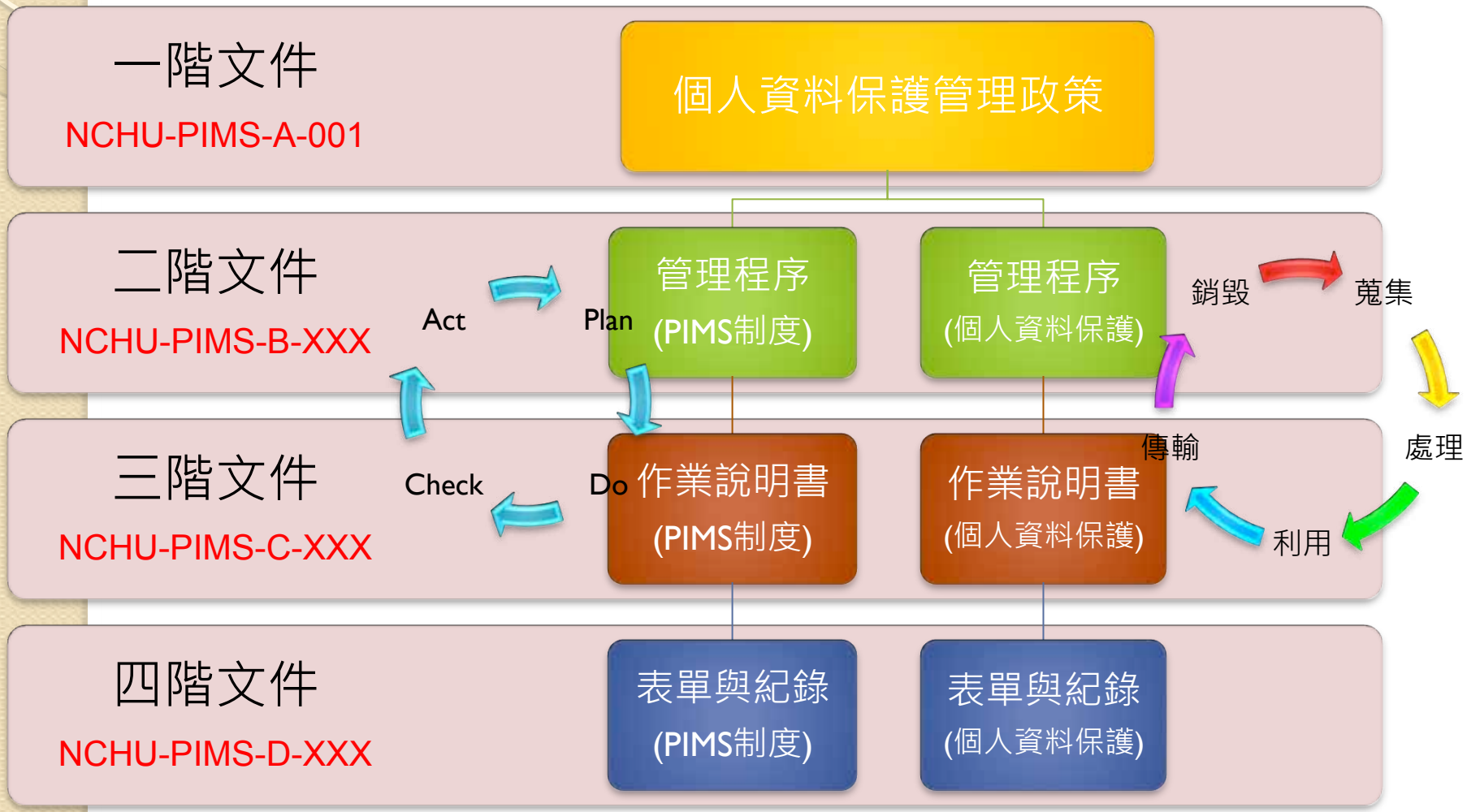
PIMS的監控與審查-3

- 6.1 矯正與預防措施
  - 6.1.1 概述
  - 6.1.2 預防措施
  - 6.1.3 矯正措施
- 6.2 持續改進

課程大綱

-
- 個人資料管理制度文件架構暨文件生命週期
-
-

個人資料保護文件架構


一階文件
NCHU-PIMS-A-001
個人資料保護管理政策
二階文件
NCHU-PIMS-B-XXX
管理程序
(PIMS制度)
管理程序
(個人資料保護)
Act
Plan
銷毀
蒐集
處理
傳輸
利用
三階文件
NCHU-PIMS-C-XXX
Check
Do
作業說明書
(PIMS制度)
作業說明書
(個人資料保護)
四階文件
NCHU-PIMS-D-XXX
表單與紀錄
(PIMS制度)
表單與紀錄
(個人資料保護)

個人資料保護文件

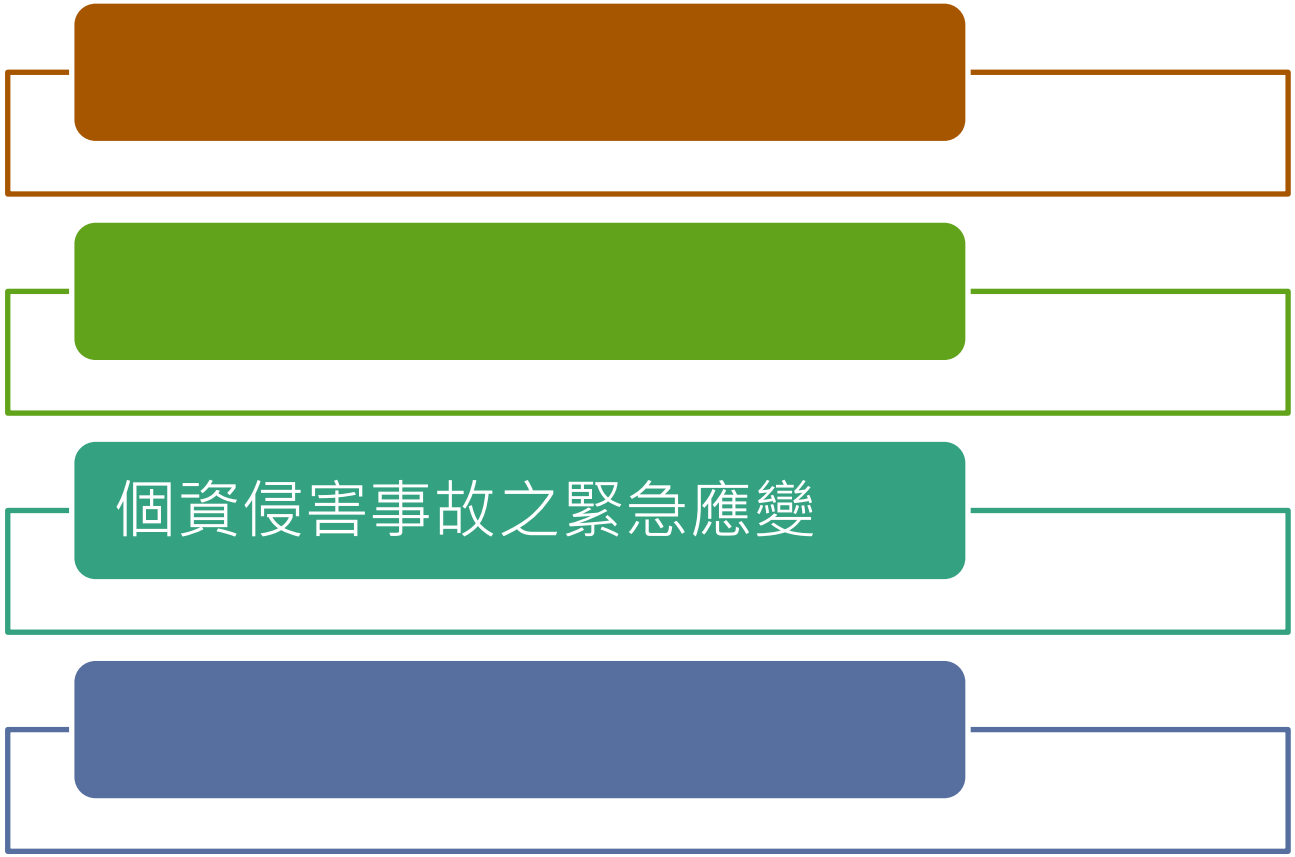
階層	PIMS文件名稱	
一階文件	個人資料保護管理政策	
二階文件	個人資料文件管理程序書	個人資料檔案風險評鑑與管理程序書
	個人資料蒐集、處理、利用與安全管理程序書	個人資料之當事人權利聲明
	個人資料稽核作業程序書	個人資料矯正預防管理程序書
	個人資料檔案安全維護計畫	業務終止後個人資料處理方法
三階文件	個人資料安全控管作業說明書	個人資料保護緊急應變處理作業說明書
四階文件	各類空白表單與紀錄	

http://www.nchu.edu.tw/notice.php?mid=442

在首頁 > 公告事項 > 本校個人資料保護與管理文件資料皆可線上下載(限中興校內網段)

個資管理文件摘要說明

課程大綱



個資外洩管道

- 問卷
- 電話客服中心
- 網購
- **掛馬網站、設計不良的網站**
- **駭客入侵**
- **社群網站**
- **P2P軟體使用**
- 銀行申請單
- 會員手冊

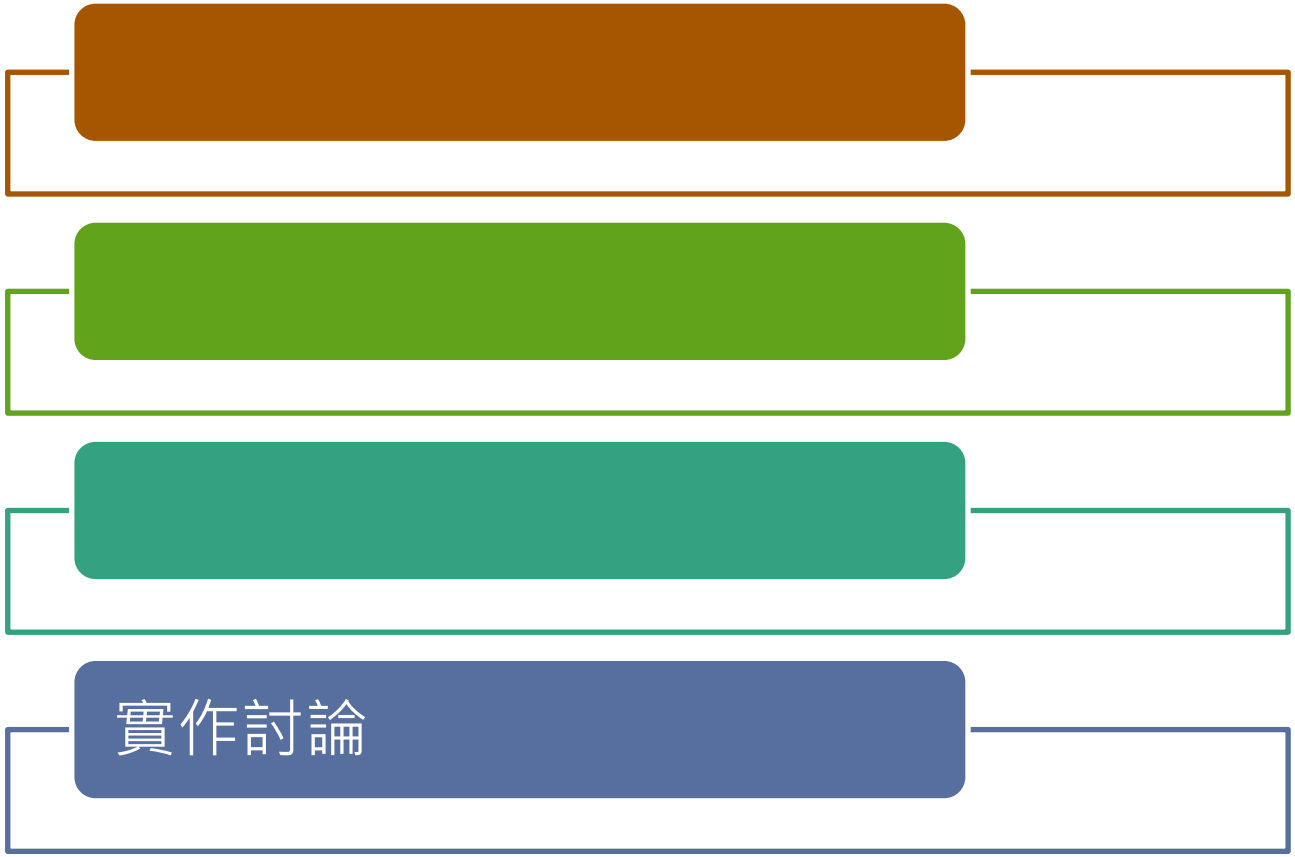
- 信用卡
- 內部人員
- 補習班
- 電子謄本系統
- 直銷公司
- 盜版光碟
- **即時通訊軟體(IM)**
- 無個資保護認知
- **釣魚網站**
- 委外廠商 *

個資外洩案例

- 扯2科大洩數百生個資
- 補教業者，假冒學生會..... 非法收集個資
- 教育單位入口網站遭駭 學生資料恐不保
- 二手硬碟轉售，個資全都露
- 國中生資料隨意丟棄校外 主管連坐罰

危機管理概要

課程大綱



應變計畫(個案範例)

個資外洩應變計畫

演練類型與方式

複雜性	演練類型	程序	頻率
低	書面審查	計畫內容審查	至少年度
中	局部計畫演練	挑戰內容	年度
中	模擬	運用情境驗證	年度或半年
中	關鍵活動演練	啟動可控制之情境，不為及營運作業	年度或低於
高	完整演練	大範圍演練	年度或低於