中興大學

個人資料管理文件教育訓練

王吉祥(Davies)
2014

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
- 個資管理文件要項
- 個資防護實務

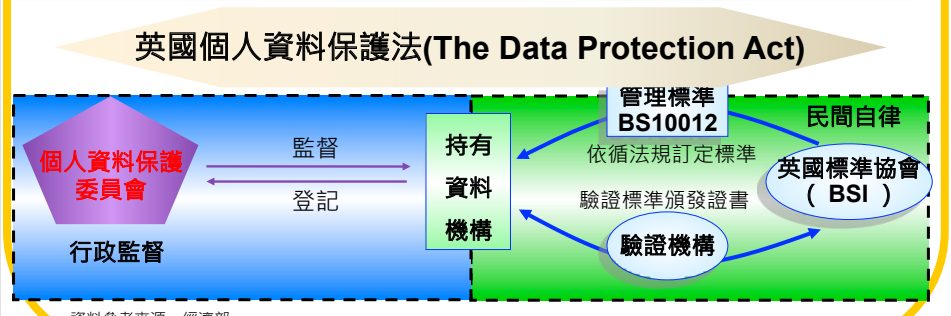
課程大綱

- BS 10012 標準暨個人資料保護法文件控管要求
-
-
-

3

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（BS10012），協助企業遵循英國個人資料保護法。



資料參考來源：經濟部

4

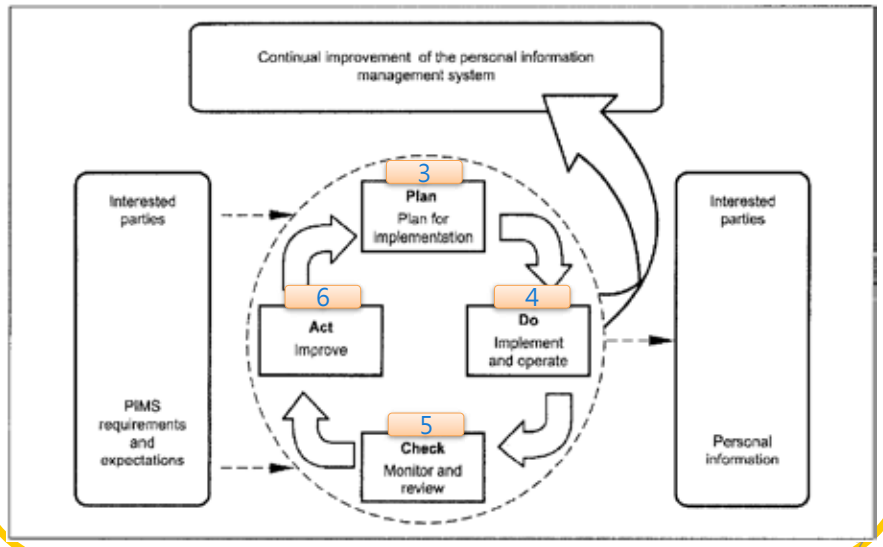
BS 10012 個人資料管理系統

- 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。

課程大綱

個人資料管理制度文件架構暨文件生命週期

Plan-Do-Check-Act (PDCA)循環



規劃個人資料管理系統-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-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

9

規劃個人資料管理系統-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.*

10

規劃個人資料管理系統-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

11

規劃個人資料管理系統-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)

12

規劃個人資料管理系統-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

13

規劃個人資料管理系統PIMS

- 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

14

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

15

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

16

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

17

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

18

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

19

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

20

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。

21

PIMS的改善

- 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

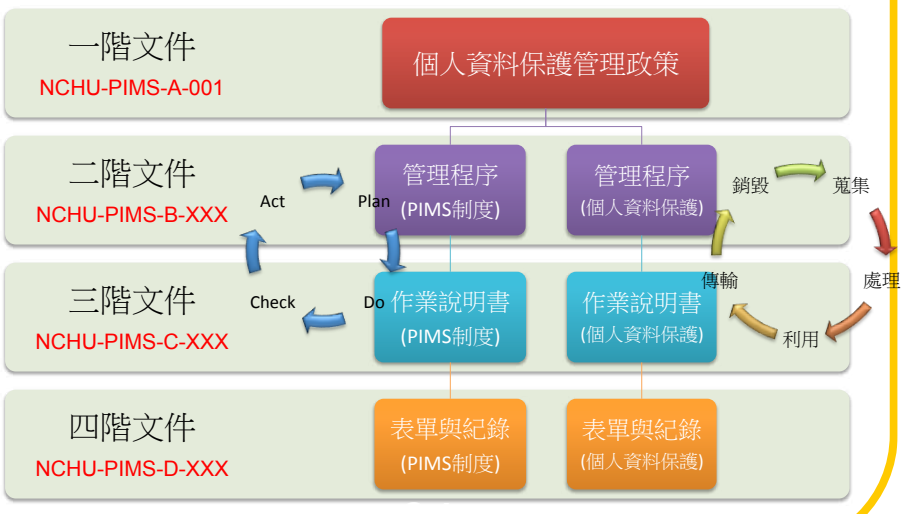
22

課程大綱

個資管理文件要項

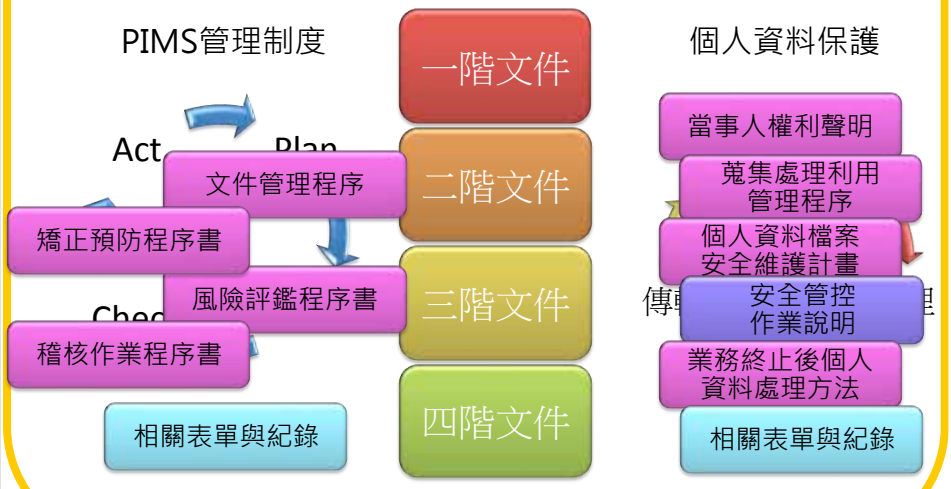
23

個人資料保護文件架構



24

個人資料保護文件說明



25

國立中興大學個人資料保護文件

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)

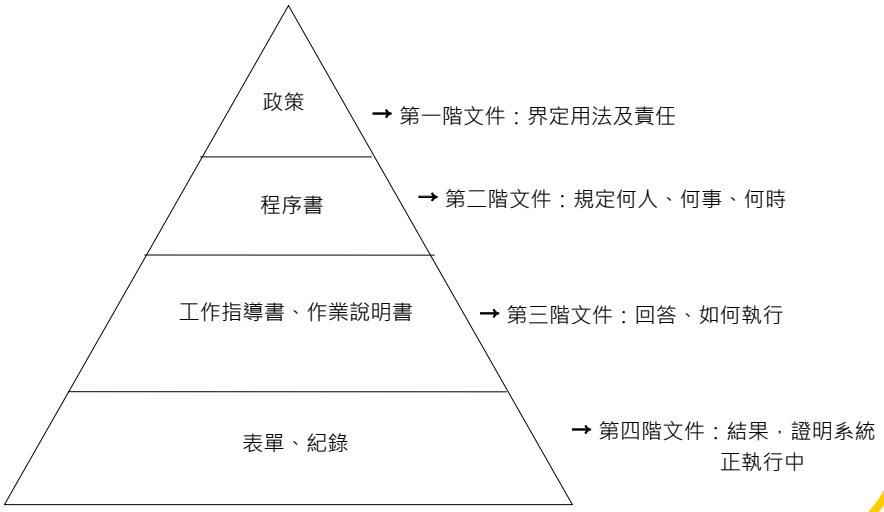
26

個人資料保護管理政策

- 政策精神
- 依據的法源與參考標準
- 適用範圍

27

個人資料文件管理程序書-1



28

個人資料文件管理程序書-2

個人資料保護管理制度文件等級分為4級;
公開使用、內部使用、內部限閱、機密。各等級之評估標準如下：

- 公開使用：無特殊之機密性要求，可對外公開之資訊。
- 內部使用：僅供組織內部人員或被授權之單位及人員使用。
- 內部限閱：僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用。
- 機密：為組織、主管機關或法律所規範之機密資訊。

29

個人資料文件管理程序書-3

文件/紀錄銷毀

- 各業務單位超過保存期限，不予保留而須進行銷毀時，應由經辦人員填寫「個人資料紀錄銷毀申請單」，經權責主管核准後，可以碎紙機絞碎或撕毀等無法回復之安全方式處理。
- 若委外執行銷毀，文件管理人員應派員監視銷毀流程，相關紀錄並附於「個人資料紀錄銷毀申請單」以留存備查。

30

個人資料檔案風險評鑑與管理程序書-1

衝擊影響程度	資產價值(衝擊值)	個人資料範圍
極高	4	自然人之姓名或國民身分證統一編號 (或護照號碼)及特種個人資料。
高度	3	一、 含自然人之姓名**及**國民身分證統一編號（或護照號碼），但不含特種個人資料。 二、 含自然人之姓名或國民身分證統一編號(或護照號碼)及財務情況（如：薪資、局帳號），但不含特種個人資料。
中度	2	(一) 含自然人之姓名或國民身分證統一編號(或護照號碼)，但不包含特種資料。 (二) 含自然人之姓名**及**員工編號(或學號)，但不含特種個人資料。
一般	1	不含自然人之姓名及國民身分證統一編號(或護照號碼)。

31

個人資料檔案風險評鑑與管理程序書-2

個人資料檔案風險值計算

- 評估個人資料檔案威脅及弱點對構面因子所產生之影響，計算出風險值。
- **風險值** = 資產價值（衝擊值）×（構面值1 × 權重 + 構面值2 × 權重 + 構面值3 × 權重）。

風險評鑑報告產出

- 上述評估資料之風險值由資安暨個資保護執行小組彙整後產出「個人資料檔案風險評鑑彙整表」。
- 依據個人資料檔案風險評鑑結果撰寫個人資料檔案風險評鑑報告，並由資安暨個資保護執行小組提出可接受之風險等級建議。

個人資料檔案風險管理：決定可接受風險值

- 本校個人資料檔案風險評鑑之可接受風險值，需經「資訊安全暨個人資料保護推動委員會」開會決議，並記載於會議紀錄中。
- 除決定可接受風險值外，亦可訂定風險處理之補償條件，篩選出可接受風險值以下，但仍須進行風險處理之個人資料檔案項目。

32

個人資料檔案風險評鑑與管理程序書-3

風險處理計畫執行成效暨殘餘風險處理

- 風險處理計畫於預訂完成日期結束後，須由資安暨個資保護執行小組(各單位聯絡窗口)執行風險再評鑑，以確認風險處理計畫執行達到風險減緩預期效益，並將風險再評鑑之結果填寫於「個人資料檔案風險評鑑彙整表」，提報管理審查會議。

風險評鑑頻率

- 每年應至少執行1次風險評鑑。
- 當作業環境、作業流程變更或系統重大異動時，應不定期執行風險評鑑。

33

個人資料蒐集處理利用管理程序

個人資料之蒐集控管原則

- 各單位使用個人資料需依個資法之特定目的必要範圍內為之，如為法定職務外、或特定目的以外之利用時，應向當事人履行告知義務，並依據個資法規定，請當事人填寫「個人資料提供同意書」取得當事人書面同意，或與當事人有契約或類似契約之關係。
- 本校相關活動之「個人資料提供同意書」及「隱私權聲明」，經該單位一級主管審查後報「資訊安全暨個人資料保護推動委員會」備查。

(詳文件)

34

個人資料當事人之權利聲明-1

本校各單位接獲申請時，應依規核對當事人身分（例如請當事人出示雙證件）。

- 受理之單位應依據【個人資料文件管理程序書】填具「個人資料使用資訊服務申請表」，除受理之單位依職權能自行辦理外，並應將當事人之請求移交個人資料保有單位處理。
- 應依據個資法要求，主動通知當事人並填具「個人資料特定目的範圍變更需求同意書」，取得當事人之書面同意。

個人資料保有單位針對當事人請求查詢、閱覽個人資料或製給個人資料複製本時，應符合下列要求：

- 應於15日內為准駁之決定。
- 准駁期間如有必要延長時，應將其原因以書面通知請求人，且延長之期間不得逾15日。
- 應具備收受請求及做出准駁之控制與紀錄保留機制。

35

個人資料當事人之權利聲明-2

個人資料保有單位針對當事人請求補充、更正、停止蒐集、停止處理、停止利用或刪除個人資料，應符合下列要求：

- 應於30日內為准駁之決定。
- 准駁期間如有必要延長時，應將其原因以書面通知請求人，且延長之期間不得逾30日。
- 應具備收受請求及做出准駁之控制與紀錄保留機制。
- 個人資料保有單位確認當事人查詢、閱覽、複製、補充、更正、停止利用及刪除之請求為無正當理由或有個資法第十條但書及第十一條第二項及第三項但書規定之情形時，應以書面方式將拒絕其請求之原因通知當事人。
- 個人資料保有單位對受理當事人請求，應確保迅速有效地處理，並作成紀錄。
- 本校所提供之服務若含個人資料，應制定及維護隱私權聲明。
- 本校相關隱私權聲明，可參酌「隱私權政策聲明範本」修訂，此聲明應讓當事人易於取得與閱讀。

36

個人資料稽核作業程序書

稽核人員之要求;

為確保稽核過程的客觀性與獨立性，稽核之執行應由非受稽人員擔任。可由下列方式組成稽核團隊執行稽核活動，依權責辦理各項個人資料保護稽核事務。

- 聘請外部個人資料保護顧問。
- 審定合格之稽核人員，如具有BS 10012主導稽核員訓練證書者或已接受個資內部稽核相關訓練者擔任。

個人資料管理制度內部稽核

- 個人資料管理制度內部稽核人員應定期參加個人資料保護教育訓練，以持續加強個人資料保護專業能力與查核技巧。
- 個人資料管理制度內部稽核每年至少辦理1次，並可視需要不定期舉行，當個人資料管理制度發生重大變更後，應立即執行稽核作業。
- 資安暨個資保護稽核小組應事先擬定稽核計畫，闡明稽核範圍與項目，陳核「資訊安全暨個人資料保護推動委員會」召集人核可後，方得實施。
- 內部稽核報告由資安暨個資保護稽核小組彙整後，呈報「資訊安全暨個人資料保護推動委員會」核定。內部稽核報告所列建議改善事項，應辦理追蹤複檢。

37

個人資料矯正預防管理程序書

- 受稽部門於接獲內部稽核報告後，應依據【個人資料矯正預防管理程序書】之規定實施矯正，並於十五個工作天內將該單位之缺失原因分析及擬採行之矯正與預防措施填列於「個人資料管理制度矯正預防處理單」內，經單位權責主管核定後回覆資安暨個資保護稽核小組。

38

個人資料檔案安全維護計畫

(詳文件)

39

業務終止後個人資料處理方法

- 本校個人資料檔案之保存期限，應依【個人資料檔案風險評鑑與管理程序書】辦理。

個人資料之銷毀控管原則

- 業務單位個人資料蒐集之特定目的消失或個人資料檔案保存期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料，但因執行職務或業務所必須或經當事人書面同意者，不在此限。
- 本校個人資料檔案銷毀時，應填寫「個人資料紀錄銷毀申請單」提出申請，經權責單位主管核可後，方可實施銷毀。
- 儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用，應確實刪除其所儲存之個人資料檔案。
- 紙本個人資料檔案銷毀時，若屬大量銷毀應指定專業廠商並有相關安全控管措施（如：人員全程陪同或全程錄影監控），若少量則應以碎紙機銷毀；若為電子檔案應確實刪除。

40

個人資料安全控管作業說明書

(詳文件)

41

個人資料保護緊急應變處理作業說明書-1

個人資料侵害事故之演練測試

- 「資訊安全暨個人資料保護推動委員會」每年至少從導入「個人資訊管理系統」標準之單位指派一單位（以下稱導入單位）執行一次緊急應變演練，以確保緊急應變計畫之正確性及有效性。

訂定演練模式及週期

- 導入單位個人資料侵害事故之演練測試，應依個資作業流程業務重要性，擬定個資作業流程演練時程表執行演練，以確保有效性並訂定演練計畫，含演練範圍及交易內容，決定該年度之測試範圍及標的。個人資料侵害事故之緊急應變計畫之演練可擇以下一種或數種測試模式：
  - 書面模擬演練(Desktop Exercise)(無法進行實況演練者)。
  - 資料回復演練(Data Recovery)。
  - 情境模擬演練(Scenario Simulation)。
  - 實況演練(Simulation)。
  - 預警/無預警演練。

42

個人資料保護緊急應變處理作業說明書-2

演練計畫包含以下項目：

- 演練目的與範圍。
- 演練情境說明。
- 演練時程規畫。
- 演練順序及步驟。
- 演練所需資源清單。
- 參與單位及負責人員清單。
- 協力廠商聯絡清單。
- 模擬通報機制。

演練測試預備會議

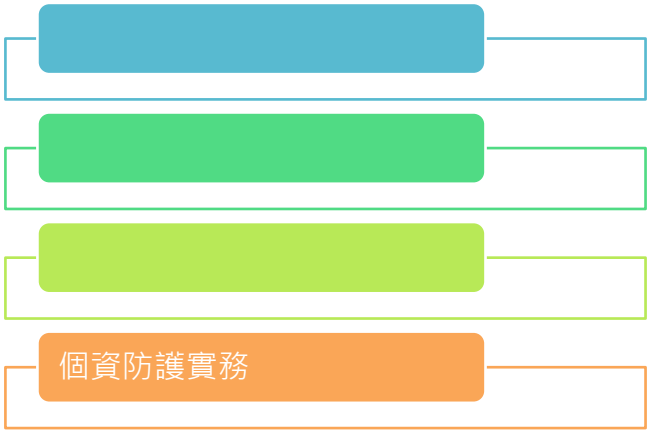
- 導入單位應於演練前召開會議，協調演練人員，說明演練內容及演練方式。

演練計畫之執行

- 演練過程中，應留存下列紀錄：
  - 模擬通報機制、啟動備援機制之過程與時間點。
  - 演練步驟(含操作指令)。
  - 演練步驟執行時間。
  - 各步驟執行之人員。
  - 各步驟執行結果。
  - 演練過程、各步驟發生之問題記錄。

43

課程大綱



44

個資保護，你可以作什麼？-1

- 個人資料檔案應**定期備份**，並防止個人資料被竊取、竄改、毀損與滅失。

- 個人資料輸入、輸出、更新或註銷時，**應該釐定使用範圍，以及調閱或存取的權限**。

- 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識之登入通行碼。個人資料檔案使用完畢後，應即退出應用程式，不得留置與電腦中。

- 含有個人資料的紙本，運用於申請、列印、存檔、轉交及銷毀等行為，**應建立相關之授權、監督及行為記錄的機制**。

個資保護，你可以作什麼？-2

- 內部傳遞或其他機關交換個人資料時，應在實體文件密封袋上，加上彌封，或對電子資料檔案壓縮加密，並加以記錄檔案的流向。

- 對於調閱個人資料的人，加以**記錄其調閱身分及行為**。調閱紀錄可視機關實際需求存檔，以利後續人員查詢及追蹤。

- 單位管理之網站或網頁內容，於確有必要公佈個人資料時，**須經所屬單位主管核准，且依相關法律及規範處理**，才能公佈。

個資保護，你可以作什麼？-3

專人處理
- **應指定專人**負責管理儲存個人資料的設備及設施，並檢查、處理設備的異常事件。

安全隔離
- 儲存個人資料的設備，**應置放於安全區域**，例如：門禁控管的辦公區域、機房等，避免有心人士或非授權人員存取。

委外監督
- 外部人員及個人，更新或維修電腦設備時，應**指派專人在場**，確保個人資料之安全，以及防止個人資料外洩。

徹底刪除
- 儲存個人資料之電腦或相關設備，如需報廢或移轉他用時，**應確實刪除該設備所儲存的個資檔案**。

個資防護實務

個資保護管理要訣：
- ✓ 人員意識
- ✓ 內部權責區隔
- ✓ 資料分權原則
- ✓ 最小儲存原則
- ✓ 資料加密原則
- ✓ 最小揭露原則
- ✓ 資料遮隱原則
- ✓ 實體安全
- ✓ 設備與媒體管理
- ✓ 委外廠商管理
- ✓ 不公務家辦

聯絡資訊

王吉祥 講師暨資深經理
+886 970 350 128
dvings@gmail.com