個人資料保護實務

楊峻榮
yang@mail.ncku.edu.tw

大綱

- 個人資料保護法概要
- 個人資料保護之管理系統
- 組織成員因應作為

個人資料保護法概要

個人資料與個人資料檔案

- 個人資料：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、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及 其他得以直接或間接方式識別該個人之資料。
  - 單一欄位是否形成"個資"？
  - 其他不含姓名之欄位組合，是否形成"個資"？
- 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式 檢索、整理之個人資料之集合。
  - 非資訊系統之儲存體檔案。

個人資料保護法架構

第一章 總則(14)	目的、定義、當事人權利、委外、書面同意、告知義務、通知
第二章 公務機關對個資的蒐集處理利用(4)	特定目的、資訊公開、安全維護事項
第三章 非公務機關對個資的蒐集處理利用(9)	特定目的、國際傳輸、行政檢查、安全維護事項
第四章損害賠償與團體訴訟(13)	民事賠償責任與團體訴訟
第五章罰則(10)	刑事及行政處罰
第六章 附則(6)	其它相關規定

個人資料之蒐集、處理與利用

- 有關醫療、基因、性生活、健康檢查及犯罪前科（特種個資)之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在 此限：
  - 法律明文規定。
  - 公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。
  - 當事人自行公開或其他已合法公開之個人資料。
  - 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料。
  - 前項第四款個人資料蒐集、處理或利用之範圍、程序及其他應遵行事項之辦法，由中央目的事業主管機關會同法務部定之。

個人資料之蒐集、處理與利用(續)

- 個資法第十五條：公務機關對個人資料之蒐集或處理，除第六條第一項(特種個資)所規定資料外，應有特定目的，並符合下列情形 之一者：
  - 執行法定職務必要範圍內。
  - 經當事人書面同意。
  - 對當事人權益無侵害。

個人資料之蒐集、處理與利用(續)

- 個資法第十六條：公務機關對個人資料之利用，除第六條第一項所規定之資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：
  - 法律明文規定。
  - 為維護國家安全或增進公共利益。
  - 為免除當事人之生命、身體、自由或財產上之危險。
  - 為防止他人權益之重大危害。
  - 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定 之當事人。
  - 有利於當事人權益。
  - 經當事人書面同意。

個人資料之蒐集、處理與利用(續)

- 個資法第十七條：公務機關將下列事項公開於電腦網站，或以其他適當方式供公眾查閱，其有變更者，亦同：
  - 個人資料檔案名稱。
  - 保有機關名稱及聯絡方式。
  - 個人資料檔案保有之依據及特定目的。
  - 個人資料之類別。
- 個資法第十八條：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。

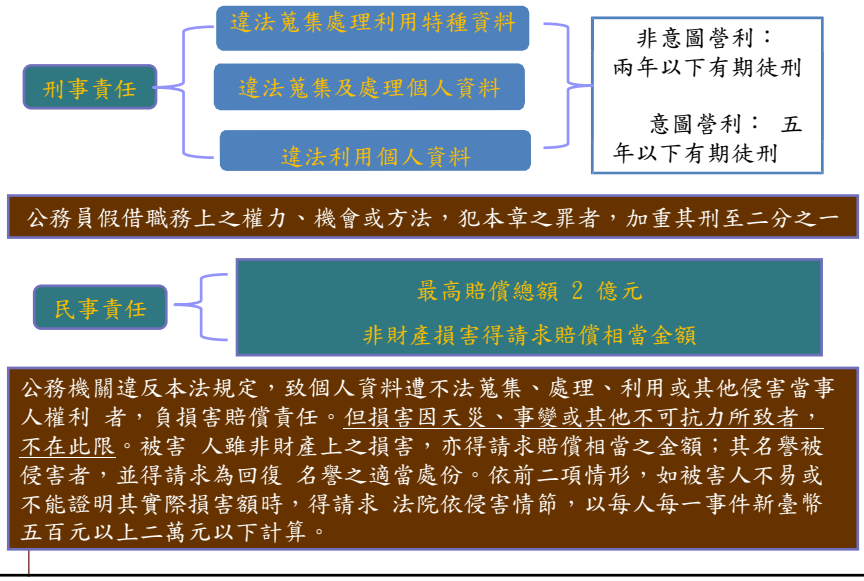
個人資料之蒐集、處理與利用-非公務機關

- 個資法第十九條：非公務機關對個人資料之蒐集或處理，除第六條第一項所規定 資料外，應有特定目的，並符合下列情形之一者：
  - 法律明文規定。
  - 與當事人有契約或類似契約之關係。
  - 當事人自行公開或其他已合法公開之個人資料。
  - 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處 理後或蒐集者依其揭露方式無從識別特定之當事人。
  - 經當事人書面同意。
  - 與公共利益有關。
  - 個人資料取自一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更 值得保護之重大利益者，不在此限。
- 蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或 利用時，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。

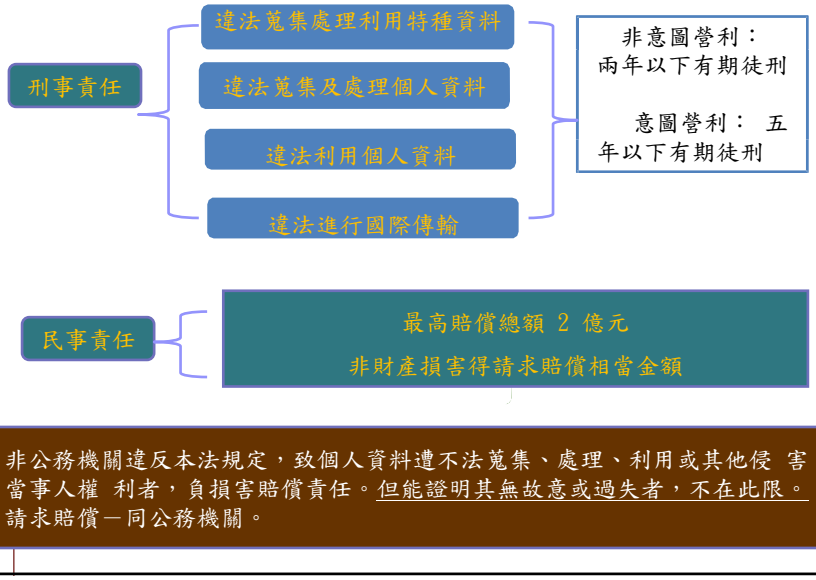
個人資料之蒐集、處理與利用-非公務機關

- 個資法第二十一條：非公務機關對國際傳輸個人資料，而有 下列情形之一者，中央目的事業主管得限制之：
  - 涉及國家重大利益。
  - 國際條約或協定有特別規定。
  - 接受國對於個人資料之保護未有完善之法規，致有損當事 人權益之虞。
  - 以迂迴方式向第三國（地區）傳輸個人資料規避本法。

罰則-公務機關



罰則-非公務機關



非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵 害當事人權 利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。請求賠償一同公務機關。

個資法施行細則第十二條之措施

- 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：

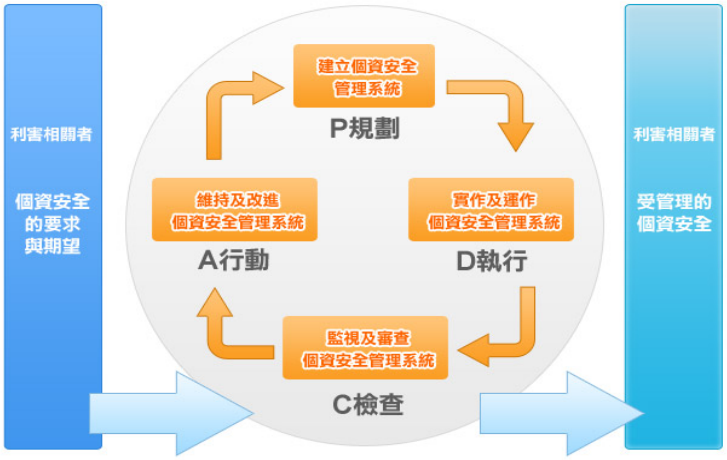
一、配置管理之人員及相當資源。
二、界定個人資料之範圍。
三、個人資料之風險評估及管理機制。
四、事故之預防、通報及應變機制。
五、個人資料蒐集、處理及利用之內部管理程序。
六、資料安全管理及人員管理。
七、認知宣導及教育訓練。
八、設備安全管理。
九、資料安全稽核機制。
十、使用紀錄、軌跡資料及證據保存。
十一、個人資料安全維護之整體持續改善。

個人資料保護之管理系統

建立個資管理制度

- 依據個資法施行細則第十二條
  - 技術性與適法性。
    - 法規要求一定要納進去。
- 考量要點
  - 適法性
    - 是否符合個資法之要求。
    - 個資法及其他法源之位階。
  - 組織規模與組織文化。
    - 推行難易度。
  - 可應用的資源。
    - 人力及技術資源
  - 領導階層之態度。

個人資料管理系統(PIMS)之PDCA



個資PDCA

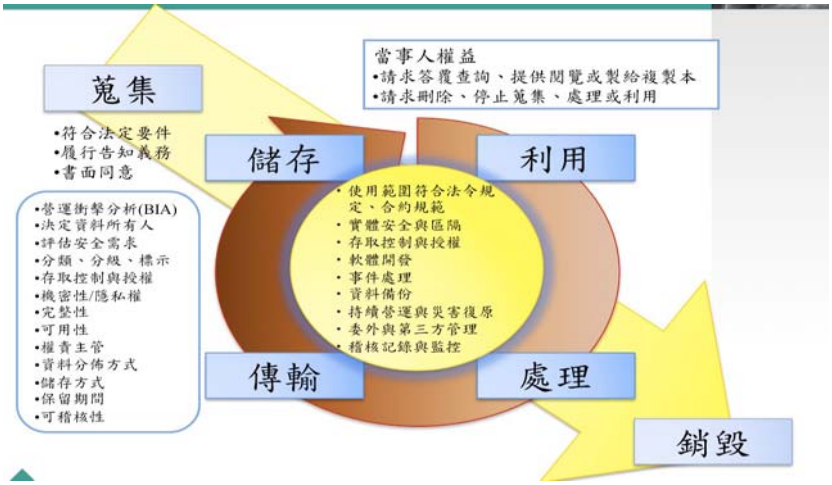
- 規劃(P)
  - 建立個人資料保護管理政策。
  - 建立管理組織架構及程序文件。
  - 建立與維護個人資料檔案清冊。
  - 確認個人資料之蒐集與利用符合法令規定。
- 執行(D)
  - 依管理程序文件執行。
- 檢查(C)
  - 組織應定期執行稽核作業，以確保相關管理措施之 有效性。
- 改善行動(A)
  - 針對資訊安全或個資事件及稽核缺失應訂定改善行動或預防措施，以減低事件再次發生機會。

個人資料保護管理措施架構

- 配置管理之人員及相當資源
- 界定個人資料之範圍
- 個人資料之風險評估及管理機制
- 事故之預防、通報及應變機制
- 個人資料蒐集、處理及利用之內部管理程序
- 資料安全管理及人員管理
- 認知宣導及教育訓練
- 設備安全管理
- 資料安全稽核機制
- 使用紀錄、軌跡資料及證據保存

個人資料安全維護之整體持續改善

定義規範－由個資的生命週期



配置管理之人員及相當資源

- 高層承諾提供資源。
- 組織成立個資執行小組
  - 執行長。
  - 執行秘書。
  - 連絡窗口。
  - 各單位個資負責人。
  - 執行之任務編組
    - 管理審查委員會。
    - 稽核小組。
    - 應變小組。

界定個人資料之範圍

- 個人資料盤點其目的除做為風險管理之標的之外，尚可由盤點做業來審視：
  - 不需保留而保留之個資檔案，不需保留而保留之記錄。
  - 是否過度收集。
- 公務機關因應法規要求公開保有個資項目：
  - 個人資料檔案名稱。
  - 保有機關名稱及聯絡方式。
  - 個人資料檔案保有之依據及特定目的。
  - 個人資料之類別。

個人資料盤點管制

- 由權責人員(個人資料之搜集者)填寫所負責業務保存之個人資料由業務流程或保存位置盤得。
- 什麼個資檔案型態須盤點管制。
  - 檔案或表單(含紙本)上含有姓名加上其他欄位足以辨識出個人者則須盤點
  - 若僅為組織內姓名及公務電話或公務電子信箱之檔案，因屬公務執行需公開之項目，不需盤點管制(目前本校預計做法)
  - 個人通訊錄屬個人行為不需盤點管制，業務所需之通訊錄且非上一項所述則需盤點管制(目前本校預計做法)

個人資料之風險評估及管理機制

- 流程
  - 以個資盤點所得為風險評估並算出風險值。
  - 決定統一之可接受風險。
  - 高於可接受風險之個資施以風險改善計劃。
  - 預計風險改善計劃之項目執行風險再評估。
- 自定風險評估之方法論，以期得出正確合理之風險高低，進而將有限資源投入高風險項目。

風險評估依個資之生命週期為考量

- 蒐集時之風險
  - 適法性，告知之責任。
- 處理時之風險
  - 應用系統處理、驗證。
- 儲存時之風險
  - 儲存設備之安全。
- 利用時之風險
  - 適法性，告知之責任。
- 國際傳輸時之風險
  - 適法性，告知之責任。
- 銷毀時之風險

風險評估方式

- 目前本校預計是以下列為風險評估之構面，由各評估值經加權公式算出一風險值。

評估項目(構面)	評估值			
	1	2	3	4
個資屬性	僅有識別資料，未含其他個人活動。	含有個人活動資料(多個當事人之資訊欄位)	含有個人活動資料及敏感資料(成績、帳號、政治傾向)	含有特種個人資料
個資記錄數量	20筆以下	21~500筆	500~20,000筆	20,000筆以上
個資生命週期之評估	涉及項目不多且皆依各步驟程序落實執行	涉及項目不多，且部份未依各步驟程序落實執行	涉及項目多但部份未依各步驟程序落實執行	涉及項目多,且多未依各步驟程序落實執行
蒐集及利用範圍	已取得當事人同意蒐集、處理，並於特定目的範圍內利用	未取得當事人同意蒐集(間接收集)、處理，但於特定目的範圍內利用	已取得當事人同意蒐集、處理，但於特定目的外之利用	未取得當事人同意蒐集、處理，並於外部利用
風險發生之機率	幾乎不可能發生	只有在特殊的情況下會發生	有些的情況下會發生	在大部份的情況下會發生

事故之預防、通報及應變機制

- 組織須建立一套處理機制，針對：
  - 當發現潛在威脅時，如何處理。
  - 當發生資安事件時，如何處理。
  - 當發生個資外洩事件時，如何處理。
  - 當發生個資告訴、抱怨事件時如何處理。
- 其目的在於控制損害及防範未然，並由錯誤中學習。
- 處理過程應記錄並注意適法性。
- 最高原則：大事化小，小事化無。

個人資料蒐集、處理及利用管理程序

- 應制定個人資料蒐集、處理及利用管理程序及其所需之表單或修改現有之表單，以符合法規之要求，如下例：
  - 確認蒐集個人資料之特定目的或具備法令所要求之特定情形或其他要件。
  - 依據資料蒐集之情況，採取適當之告知方式或是否得免告知。
  - 確認是否得進行及如何進行特定目的外利用，欲新增或變更特定目的時，如何處理。
  - 委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人為適當之監督
  - 蒐集、處理及利用特種個人資料，符合相關法令之要求。
  - 確認其所保有之個人資料處於正確且最新之狀態。
  - 提供當事人行使權利之方式及 確認當事人身分之方式。

同意書內容範例

本同意書說明國立成功大學（以下簡稱本校）將如何處理本表單所蒐集到的個人資料。當您勾選「我同意」並簽署本同意書時，表示您已閱讀、瞭解並同意接受本同意書之所有內容及其後修改變更規定。若您未滿二十歲，應於您的法定代理人閱讀、瞭解並同意本同意書之所有內容及其後修改變更規定後，方得使用本服務，但若您已接受本服務，視為您已取得法定代理人之同意，並遵守以下所有規範。

一、 基本資料之蒐集、更新及保管

1. 本校蒐集您的個人資料在中華民國「個人資料保護法」與相關法令之規範下，蒐集、處理及利用您的個人資料。

2. 請於申請時提供您本人正確、最新及完整的個人資料。

3. 本校因執行業務所蒐集您的個人資料包括姓名、職稱、聯絡方式(電話、E-Mail)等(視狀況，自行調整)。

4. 若您的個人資料有任何異動，請主動向本校申請更正，使其保持正確、最新及完整。

5. 若您提供錯誤、不實、過時或不完整或具誤導性的資料，您將損失相關權益。

6. 您可依中華民國「個人資料保護法」，就您的個人資料行使以下權利：

(1) 請求查詢或閱覽。(2)製給複製本。(3) 請求補充或更正。(4) 請求停止蒐集、處理及利用。(5) 請求刪求。但因本校執行職務或業務所必須者，本校得拒絕之。若您欲執行上述權利時，請參考本校之個人資料保護聯絡窗口聯絡 方式與本校連繫。但因您行使上述權利，而導致權益受損時，本校將不負相關賠償責任。

二、 蒐集個人資料之目的

1. 本校為執行電子郵件申請業務(視實際狀況，各表單自行調整)需蒐集您的個人資料。

2. 當您的個人資料使用方式與當初本校蒐集的目的不同時，我們會在使用前先徵求您的書面同意，您可以拒絕向本校提供個人資料，但您可能因此喪失您的權益。

3. 本校利用您的個人資料期間為即日起 10 年內(視實際狀況，各表單自行調整)，利用地區為台灣地區。

□我已閱讀並接受上述同意書內容　　當事人簽名 **(請親簽)**　　年　　月　　日

資料安全管理及人員管理

- 定義蒐集、處理及利用個人資料之各相關業務流程之負責人員。
- 定義所屬人員不同之權限並控管之。
- 與所屬人員簽訂保密契約，契約內容至少包含所屬人員應負之保密義務與保密範圍，及違反保密義務之效果。
- 確保資料之安全，如傳輸之安全-加密及儲存之安全－備份。
- 委外之管理。
- 認知宣導及教育訓練。
- 業務移交。

設備安全管理

- 目標－防範非法存取及資料外洩。
- 利用電腦或相關設備蒐集、處理或利用個人資料時，採取之技術管理措施。
- 視需要設置安全系統，如防火牆，防毒軟體等。
- 系統更新之控管。
- 紙本及可攜式儲存媒體之控管。

資料安全稽核機制及持續改善

- 為確保本制度之有效性、符合性，應定期稽核本制度是否落實執行。
- 為持續改善本制度，應建立下列程序（矯正預防）：
  - 稽核時發現未落實執行之情形時之改善。
  - 發生事件後之改善措施。
  - 發現潛在問題之改善。

稽核作業表

查核項目	自我評審			稽核評量結果			
				完整性			
	是	否	不適用	非常	尚屬	不盡	不適用
2 個人資料保護與安全							
2.1 是否指定機關副首長為個資隱私業務之機關召集人？	□	□	□	□	□	□	□
2.2 是否指定專人依法令規定辦理安全維護及保管事項？	□	□	□	□	□	□	□
2.3 是否設置「個資保護聯絡窗口」，協調聯繫個資事宜，並將聯繫方式（如：電話、email）置於單位網站，以便利民眾提出申訴與救濟？	□	□	□	□	□	□	□
2.4 個人資料之處理行為是否經權責單位核准，釐定使用範圍及調閱、存取權限？	□	□	□	□	□	□	□
2.5 個人資料之處理行為是否留存使用者身分與其行為紀錄以供事後稽查？	□	□	□	□	□	□	□
2.6 含有個人資料之紙本報表，其處理及利用行為是否有適當之授權、監督，及記錄列印、轉交等行為？	□	□	□	□	□	□	□
2.7 交換紙本個人資料時，是否採取彌封或其他具備保密機制之傳遞方式？	□	□	□	□	□	□	□
2.8 交換個人資料時，是否記錄轉交或傳輸行為之流向？	□	□	□	□	□	□	□
2.9 對於個人資料之調閱，是否有申請及核准程序？	□	□	□	□	□	□	□
2.10 對於個人資料之調閱，是否記錄並保存調閱者身分及行為？	□	□	□	□	□	□	□

使用紀錄、軌跡資料及證據保存

- 考量業務之需求、設備之限制與個資之風險，評估保存下列紀錄：
  - □ 因應事故發生所採取行為之紀錄。
  - □ 確認受託人執行委託人要求事項之紀錄。
  - □ 提供當事人行使權利之紀錄。
  - □ 確認資料正確性及更正之紀錄。
  - □ 權限新增、變動及刪除之紀錄。
  - □ 違反權限行為之紀錄。
  - □ 備份及還原測試之紀錄。
  - □ 個人資料交付、傳輸、刪除、廢棄之紀錄。
  - □ 存取個人資料系統之紀錄。
  - □ 定期檢查處理個人資料之資訊系統之紀錄。
  - □ 教育訓練之紀錄。
  - □ 計畫稽核及改善程序執行之紀錄

組織成員因應作為

認知

- 詳閱個人資料保護法及施行細則條文。
- 詳閱組織之個人資料保護管理制度文件。
- 踴躍參加個資保護及資訊安全教育訓練。

個資盤點及風險評估

- 了解所負責業務流程所涉及之個資檔案，若為業務所需應盤點控管。
- 檢視資訊設備內所儲存之個資檔案
  - 暫存或已不在使用之個資檔案予以刪除。
  - 檢視個資檔案欄位是否超過執行業務所需。
  - 過期或超過保存期限之記錄給予刪除。
- 紙本
  - 過期或超過保存期限之表單給予銷毀（碎紙）。

事故之預防、通報

- 當有跡象顯現儲存個資之資訊設備或儲存個資之紙本場所疑似遭入侵或破壞，應主動通報相關人員，訂有程序者依程序通報處理。
- 已發生明顯個人資料被竊取、洩漏、竄改或其他侵害事件時，例如存有個資之可攜式儲存設備遺失或紙本遺失等，處理時應考量法規要求。
  - 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或 其他侵害者，應查明後以適當方式通知當事人。

個人資料蒐集、處理及利用

- 依個資法及組織程序書規定蒐集、處理及利用個人資料。
- 組織內其他單位調閱個人資料時應依管理制度規定辦理。
- 蒐集個人資料時請先評估業務所需，不過度蒐集，但可考量其他業務所需一併收集，唯需事先告知特定目的。

資料安全與設備安全

- 充份了解所負責之業務涉及個資的部份及其存放之位置，定期檢視個人資料之存取權限正確與否，及存取之情形。
- 做好個資保存之規劃，如存放位置與備份位置。
  - 儘量不與作業系統放同一實體硬碟。
- 含有個資之紙本應保存好，廢棄之個資紙本應碎紙，不宜直接丟垃圾桶或當背面可影印用紙。
- 個資檔案因應完整性要求應備份，但備份檔也應保護，可用加密措施。
  - 一般之壓縮打包工具皆有加密功能，如7-zip、winrar。
- 於處理個人資料之電腦系統中安裝防毒軟體，並定期更新病毒碼，及開啟防火牆。
  - Windows ： 系統預設防火牆或防毒軟體附屬之防火牆。
  - Linux： hosts.allow&hosts.deny 或 iptables
- 於處理個人資料之電腦系統中,勿裝非法或來路不明之軟體，及儘量避免當成上網之平台。
- 電腦作業系統及相關應用程式之漏洞，定期安裝修補之程式。
- 實體與電腦桌面淨空，應設定螢幕保護程式與密碼。

資料安全與設備安全(續)

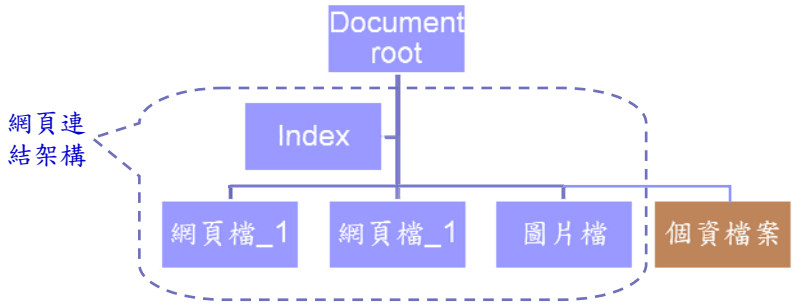
- 應經常檢查電腦系統之狀況：
  - CPU、Process、Disk等系統資源。
  - 帳號、存取等權限。
  - 相關之log（存取及系統紀錄）。
- 資訊設備送修時，應先移除保存個資之硬碟或其他儲存設備。
- 個人資料儘量避免直接存於外接儲存設備，若得儲存則應加密或加密碼鎖。
- 資訊設備應使用帳號及密碼登入，使其具備一定安全之複雜度之密碼並定期更換。
- 傳真前確認傳真處所電話及傳真內容、傳真前先與對方電話聯絡、確認傳真傳送紀錄，傳真傳出後原稿迅速回收。
- 定期刪除多功能事務機的儲存資料。
- 寄信之前再次確認寄送Email網址及寄信內容，必要時使用收送信軟體的收件者名稱檢查功能
  - Outlook / Window Live mail: 檢查名稱
- 以紙本傳送個資時雙方留存收受紀錄。

資料安全與設備安全(續)

- 在電腦、相關設備或系統上設定警示與相關反應機制，以對不正常之存取為適當之反應與處理。
  - 以mail或簡訊通知
- 測試處理個人資料之資訊系統時，不使用真實之個人資料。委外處理亦同。
  - 王○○:A123456789
- 處理個人資料之資訊系統如有變更時，確認其安全性並未降低或產生新的問題。
  - 原有系統及資料需備份。
- 在電腦、相關設備或系統上設定認證機制，對有存取個人資料權限之人員進行識別與控管，且儘可能不共用存取權限。
  - 檔案分享須設帳密。

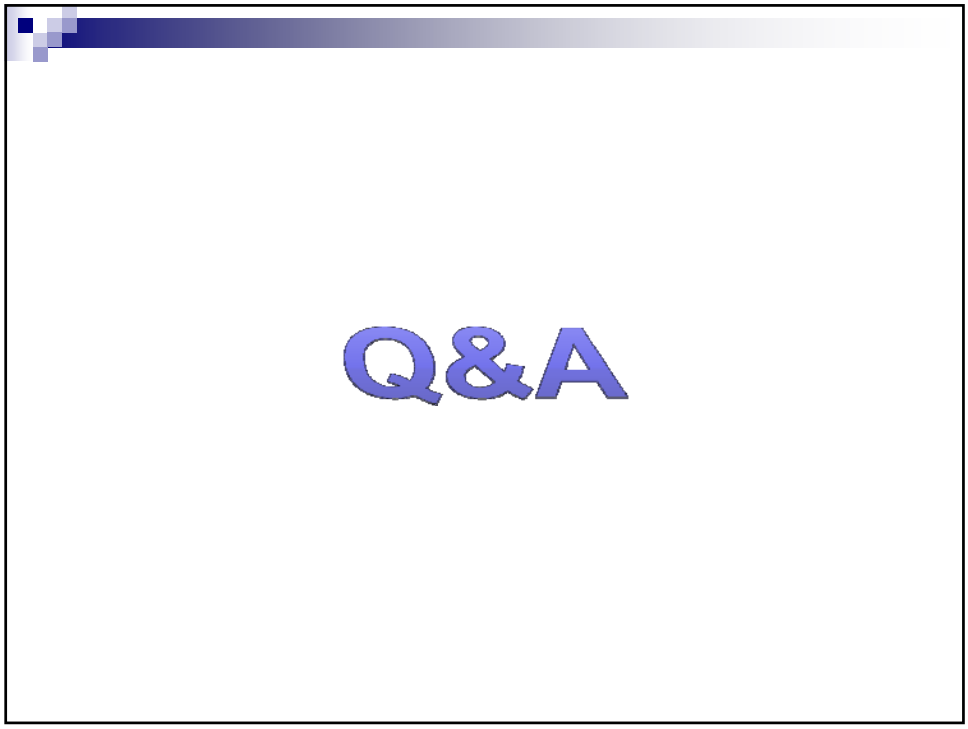
網站個資揭露

- 網頁上揭露個人資料，須經當事人同意
- 個資檔案雖不在網頁連結架構內，也有可能遭意外之揭露，如搜查引擎。



使用紀錄、軌跡資料及證據保存

- 各種個人資料管理之表單依規定保存。
- 資訊設備開啟記錄：
  - Windows
    - 控制台／事件檢視器(log位置)
    - 控制台／本機安全性原則／本機原則／稽核原則(設定)
  - Linux
    - /var/log(log位置)
    - /etc/syslog.conf (設定)
- 因應法規要求之記錄保存年限及避免log遭竄改，可建置log server 。


Q&A