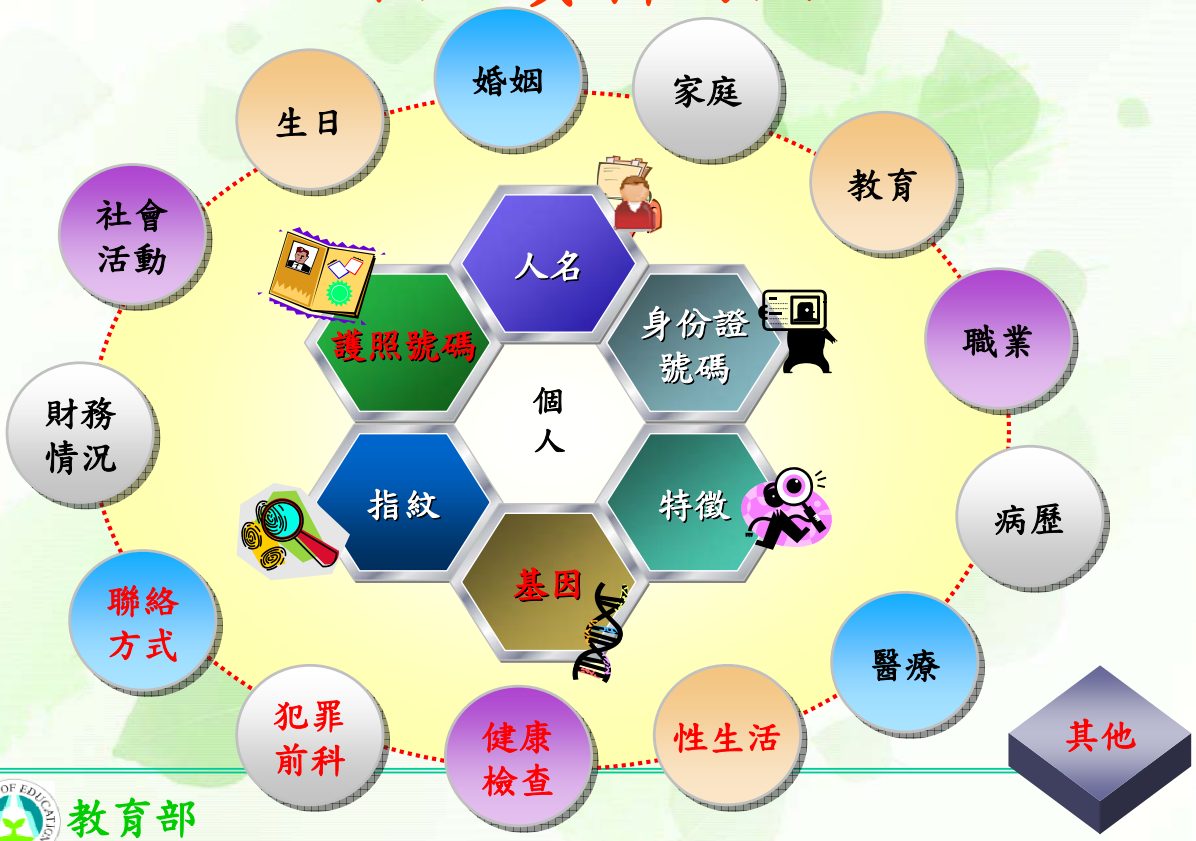
教育部資訊安全外部稽核宣導

宏瞻資訊

大綱

- 個人資料保護
- 資訊委外須知
- 公務資料攜出使用注意事項
- 自我評審檢查表
- 問題與討論

個人資料內涵



教育部

新舊個資法比較(1)

	舊版	新版
名稱	電腦處理個人資料保護法	個人資料保護法
適用行業	公務機關及八大重點行業與經指定適用之特定行業或團體 Ex:徵信業、電信業、醫院、學校、金融業、證券業、保險業、大眾傳播業 、期貨業、產物、人壽保險商業同業公會及台灣更生保護會	所有行業皆適用
保護範圍	經電腦處理之個人資料	所有個人資料(納入人工資料)

新舊個資法比較(2)

	舊版	新版
民事責任	每人二萬元至十萬元 單一事實總額最高二千萬元	每人五百元至二萬元 單一事實總額提高至二億元
刑事責任	1. 必須為因意圖營利而違法 2. 二年以下有期徒刑或併科四萬元以下罰金 3. 告訴乃論	1. 非意圖營利而違法時，得科處二年以下有期徒刑(告訴乃論)，或併科二十萬元以下罰金 2. 意圖營利而違法時，五年以下有期徒刑(非告訴乃論)，或併科一百萬元以下罰金
行政責任	限期改正、罰鍰新台幣一萬元至十萬元不等(得按次處罰)	限期改正、罰鍰新台幣二萬元至五十萬元不等(得按次處罰)

資訊委外須知

教育部委外資安管理規定

- 教育部部內訂有「教育部補助委辦採購維護伺服主機及應用系統網站資訊安全管理要點」，各單位應依規定辦理委外事務
- 資訊業務委外時，應於事前審慎評估可能的潛在安全風險，於簽訂契約條款時，納入相關資安管理規定與廠商權責。

管理要點

- 廠商應遵守本部資安規定執行工作
- 廠商與廠商人員應簽立保密合約及保密承諾書
- 發生資安事件時，廠商應依本部資安事件分級處理程序內之時限，完成事件之排除

- 資訊委外服務契約應納入之資訊安全事項
  - 涉及機密性、敏感性或是關鍵性的應用系統項目。
  - 應經核准始得執行的事項。
  - 廠商如何配合執行機關營運持續運作計畫。
  - 廠商應遵守的資訊安全規範及標準，以及評鑑廠商遵守資訊安全標準的衡量及評估作業程序。
  - 廠商處理及通報資訊安全事件的責任及作業程序。

主機系統管理

- 伺服主機應安裝主機型防火牆
- 應安裝防毒軟體並隨時更新病毒碼
- 維護時，應於加密管道進行(如SSH,SSL等)，並限制維護來源IP
- 每半年/不定期進行權限調整作業

機密性及敏感性資料之管理

- 建立機密性及敏感性資料的處理程序，以防止洩漏或不法及不當的使用
- 機敏資料之安全處理作業，應包含：
  - 建立收受機敏資料的正式收文紀錄
  - 分發對象應以最低必要的人員為限
  - 資料上明確標示資料機密等級
- 儲存機敏資料的電腦媒體，當不再使用時，應以安全的方式處理，例如：燒毀或是以碎紙機處理，或將資料從媒體中完全清除

- 機關間進行資料或軟體交換，應訂定正式的協定，並將機敏資料的安全保護事項及有關人員的責任列入
- 機關間資料及軟體交換的安全協定內容，應考量下列事項：
  - 控制資料及軟體傳送、送達及收受的管理責任與作業程序
  - 識別資料及確定軟體傳送者身分的標準
  - 資料遺失的責任及義務
  - 保護機敏資料的安全措施

應用系統(網站)管理

- 上線前
  - 應用系統應即時進行相關程式、服務軟體、資料庫系統等軟體完成弱點掃描並完成修補
  - 針對應用系統程式、資料及資料庫應進行定期備份及配合本部執行業務持續運作演練
- 上線後
  - 應用系統應定期針對相關程式、服務軟體、資料庫系統等軟體進行弱點掃描並完成中風險以上弱點之更新修補
  - 相關個資及機敏性資料提供填報或資料上載應提供加密機制

公務資料攜出使用注意事項

情境一

- 長官外出開會，忘記攜帶資料，怎麼辦?
  - Email傳輸?
  - 利用隨身碟進行資料交換?
  - 用即時通訊軟體傳送?
  - 專人遞送?

情境二

- 同仁攜帶筆記型電腦外出上課，臨時需要處理公務，該注意甚麼?
  - 電腦遺失?
  - 有心人士窺視?

資料外洩之可能途徑

- 防毒、備份與其他應用軟體之漏洞造成較大傷害
- 使用者端使用軟體之漏洞：Office、瀏覽軟體、影音播放軟體等
- 員工造訪網站
- Web應用系統漏洞
- 作業系統及服務的 Default Configuration & PSW
- 其他與資訊系統無關的資訊外洩漏洞(實體環境)

Source: SANS Top 20 Internet Security Risks of 2007 Point to Two Major Transformations in Attacker Targets , SANS

自我保護方式

- 已完成電腦系統帳號密碼設定
- 已完成螢幕保護密碼設定
- 已關閉資源分享
- 無來路不明或未授權軟體
- 已安裝防毒軟體
- 已完成瀏覽器安全設定
- 郵件軟體已關閉信件預覽
- 無eDonkey,BT,Foxy等P2P軟體
- 無Web,FTP,Mail等網路設站服務
- 已完成MS-Office軟體巨集安全設定
- Guest帳號已關閉
- 隔離機密性敏感性檔案資料
- 開啟windows系統自動更新程式
- 無閱覽不當之網站
- 是否開啟防火牆
- 重要業務文件均已備份
- 刪除瀏覽器所記憶密碼

個人電腦自我檢查表

自我評審檢查表

問題與討論