本校個資保護之推動計劃

楊峻榮

yang@mail.ncku.edu.tw

成大計網中心

大綱

- 個人資料保護概述。
- 本校個資保護措施-參照個資法施行細則第9條。
- 本校個資保護當務之急及資源需求。

個資防護之挑戰

- 組織內有多少位置存放個資
  - 如何辨識個資外洩管道。
- 個資處理揭露與業務執行之衝突。
  - 個資法對於組織政策、業務執行衝擊。
- 「適當」安全維護措施的廣度與深度。
- 組織成員的認知。
- 法規定義不明確之疑慮。

資防護基本觀念

- 個資法是法律，因應措施著眼於符合法規要求。
- 個資防護不是僅為資訊人員之責任，而是組織全體的責任。
- 個資防護之推動不是專案形式，必須持續維運。
- 組織每位成員都可能成為個資防護漏洞。
- 個資訴怨之舉證責任在於組織，故本校必須有完整個資保護措施，展現已做到良善管理之責任。
- 管理階層應提供承諾建立、完成、監督、檢視、維護及改善資安與個資管理制度之落實。

學校個資之種類

- **教職員、學生資料**
  - 姓名、電話、地址、家長姓名、學生證/身份證號碼/護照號碼。
- **校務行政資料**
  - 姓名、學生證號碼、成績單（敏感資料）、操行（敏感資料）等。
- **身心資料(特種資料)**
  - 姓名、健康及心理輔導資料記錄。
- **薪資資料**
  - 姓名、身分證字號、地址、電話、薪資、級別。
- 其他
  - 研討會、營隊報名資料。
  - 申請各種業務所填之個人資料。

個資執行與推動時程

- 先期作業階段
  - 成立組織，並賦予職責。
  - 先期會議及教育訓練。
- 導入階段(本年度10月，配合個資法預計之正式施行時間)
  - 定義規範及程序書。
  - 舉辦教育訓練。
- 執行階段(依PDCA週期)
  - 依據[個資施行細則與BS10012措施大項]所定義之程序及規範持續執行。

施行細則第9條之適當安全維護措施

- 成立管理組織，配置相當資源。
- 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。
- 必要之使用紀錄、軌跡資料及證據之保存。
- 個人資料安全維護之整體持續改善。

成立組織

- 本校必須要有專人、專責組織負責個資保護相關事宜。
- 成立個資保護執行與推動小組並定期開會，成員:
  - 執行長
    - 機關副首長:副校長。
  - 各單位代表：針對所屬單位宣導、監督
    - 各一級單位: 各學院代表及各一級單位代表。
    - 重點單位: 例如計網中心、人事室、註冊組、衛保組、心理輔導組。
  - 法律專家。
  - 專責承辦人
    - 執行個資業務承辦人員。
    - 個資申訴窗口及個資事件處理人員。

個資執行與推動小組職責

- 依法規要求或必要之安全維護措施定義規範及程序書:
  - 規範－針對本校所有成員。
  - 程序書－針對重點單位及成員。
- 舉辦教育訓練。
- 處理個資安全事件。
- 稽核各單位執行情形。
- 例行行政事務。
- 單位代表並負責單位內執行之推動及監督。

界定個人資料之範圍

- 定期進行個資盤點，必須確認個資擁有者及存放位置，包括紙本和電子個資。
- 各單位之個資清查，清查彙整後公告。
- 依資料之重要性與敏感性定義等級
  - 重點單位：
    - 人事室、教務處、衛保組、心輔組、計網中心。
  - 一般單位系所也有保護個資之責任。

個人資料之風險評估及管理機制

- 評估風險: 依個資之敏感度及威脅定義其風險值。
- 管理風險:施以風險改善計劃以降低其風險。
- 類似ISMS之風險評估及管理機制。

事故之預防通報及應變機制

- 針對個資之外洩、遭竄改之事件之處理及通報程序。
- 含外來訴怨之程序。

個人資料蒐集、處理或利用之程序

- 制定出個人資料保護相關的執行程序與標準作業流程
  - 蒐集
    - 依法進行告知義務。
    - 取得書面同意。
  - 處理
    - 儲存
      - 採取適當保護措施，避免個人資料遭竊取、竄改或毀損。
    - 銷毀
      - 特定目的消失或期限屆滿。
      - 當事人要求。
      - 處理設備或紙本銷毀。
  - 利用
    - 應於蒐集之特定目的內使用。
    - 特定目的外之使用應另外取得書面同意。
- 含當事人行使權利之處理程序 – 個人對於個資都有閱覽查詢權力。

資料安全管理及人員管理

- 定義電子資料及紙本資料之安全控管程序。
- 針對處理個資資料之人員定義其規範及獎懲措施。

人員管理及教育訓練

- 教育訓練項目
  - 個資概念與法律。
  - 個資保護措施。
- 教育訓練類別
  - 學生：納入通識教育。
  - 主管。
  - 重點單位人員。
  - 一般人員。

資訊系統與設備保護

- 計網中心:導循目前實施之ISMS規範。
- 其他單位:針對其他單位處理個資之資訊系統訂定資安規範。

資料安全稽核機制

- 針對各單位之個資安全控管定期進行稽核。
- 若導入BS10012:2009之PIMS規範，則依個資法及PIMS規範進行稽核。
- 若未導入BS10012:2009，則依check_list方式查核其符合性或有效性。

記錄與證據之保存

- 處理個資之記錄須保存及保護。
- 資訊設備或者紙本資料之個資存取控制的記錄、日誌檔（Log）等，都必須完整保留及適當的保護。
- 建置log server收集記錄統一控管。

個資安全維護之整體持續改善

- 透過稽核結果、預防措施與矯正行動以及管理階層審查，持續改善個資管理措施之有效性。
- 經由訴怨、安全事件、及其他議題來協助改善改善個資管理措施之有效性。

其他措施

- 技術上安控措施
  - 弱點掃瞄。
  - 個資掃瞄。
  - 個資存取監控中心。
- 其他安全維護事項 – 概括條款，補草案規劃上有其他不足之處的補充法源依據。

本校當務之急-1

- 先期作業階段: 目前該做而未做。
- 人力資源-專人專職負責個資保護之業務。
- 成立執行推動組織
  - 進行推動作業，並成立各工作小組
    - 如稽核小組，事件處理小組。
- 評估是否委外導入個資管理系統（PIMS）
  - 由顧問公司協助導入BS10012。
  - 包含規範程序之制定、教育訓練、稽核驗證。

本校當務之急-2

- 個資保護之先期作業，雖個資法施行細則尚未施行，但有些已確認或急迫性措施應先執行(由推動小組主導)：
  - 已確認之法規要求
    - 教育訓練及宣導。
    - 現有作業針對法規要求做必要之修正，如申請單加上收集資訊之聲明。
    - 檢視不必要之個資(含作業暫存檔)給予刪除。
    - 公開揭露(如網頁)之個資，補行告知同意。
  - 補強已執行之措施
    - 重新檢視個資清冊。