BS10012風險評鑑教育訓練

淡江大學 資訊處 教學支援組
組長 林東毅 (2018)

本文件建議印表方式:
雙面列印、每面印4頁,
本文件可使用省碳模式列印,敬請愛惜地球資源,盡量不要印表

風險評估概念說明

- 你要投保那些東西? (資產盤點)(個資盤點)
- 這些東西(含人)本身價值,評估出來值多少錢?(資產價值)(個資檔案價值:機密性等級,數量多寡)
- 你本身(設備)有哪些疾病的(內在弱點),
- 那你還會從事哪些活動可能會造成理賠(外在威脅),
- 那你如何保護自己,降低理賠發生的可能 (控制措施)

- 評估結果是否精確,仰賴方法論的好壞與評估人員的熟練度.(沒有絕對好或不好)

本校風險評估配合BS10012:2017標準調整內容

盤點表:

1. Phase I 表:刪除盤點日期欄位,僅留整體盤點日期
2. Phase II表:部分欄位位置調整,部分欄位名稱與備註說明修改(大部分盤點項目沒有異動).
3. 可還原的去識別化資料需做個資盤點與風險評估.

風險評估表:

1. 部分個資類別欄位名稱變更,並增加個資項目.
2. 個資類別欄位:指紋移到特種個資, 原欄位變更為數位識別資料(包括網路位置、GPS定位、網路代號…),但是線上即時聯絡方式line、FB、WeChat…等仍是高風險個資.

本校風險評估配合BS10012:2017標準調整內容

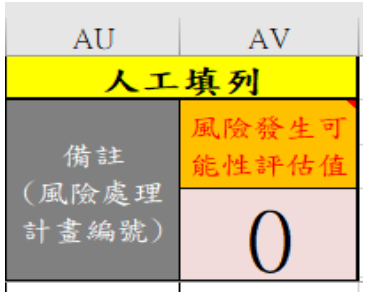
3. 特種個資:加入生物特徵(基於唯一識別自然人為目的生物資料，例如指紋、人臉辨識)
4. 高風險個資:加入國家證號、兒童、弱勢、監護人。
5. 新增excel工作表「8.隱私衝擊加權」、「9.風險發生可能性加權」。(此表單請勿修改)
6. 風險評估加入隱私衝擊評估考量、風險發生可能性評估，風險值計算方式修正與更新。

新版盤點表與風險評估表建議更新步驟

1. 先將舊表單備份一份
2. 先不要調整內容直接做新舊表資料搬移,再修正內容
3. 盤點表:
   - 「 Phase I 表」:將舊表盤點日期欄刪除後,直接COPY到新表
   - 「 Phase II表」:將舊表欄位位置有變動的資料(B欄-M欄),分別COPY到新表相同欄位中,其餘欄位資料(N欄-AO欄)一次選取直接copy到新表相同欄位中。(check一下)

新版盤點表與風險評估表建議更新步驟

1. 3.風險評估表:
   - 「 1.建議控制措施列表」：
     只新增第66項,第1-65項的已建置及未建置選項,可直接從舊表COPY過來.
   - 「 3.風險評估彙總表」：
     - 直接從新盤點表相同欄位(E欄-I欄) copy到新風險評估彙總表(A欄-E欄)中,再從舊風險評估彙總表(G欄-AC欄)COPY到新表(F欄-AB欄). (check一下)
     - 新增欄位「風險發生可能性評估值」(AV欄): 為最近一年各單位不符合事項+觀察事項+改善機會個數+個資洩漏次數總和.(以一級單位各自填表統計)



- 4.依現況修正盤點表與風險評估內容.

注意事項

- 控制措施統一作法?
  80%該建置之控制措施,均已建置,才能勾選已建置
- 各單位修改風險評鑑資料完成後,請提報一級單位存查與追蹤

常見問題

- 單位之工作流程未全部列出
- 個資筆數算法錯誤
- 一級單位內,相同的個資檔案,流程不同,評估方法也不同
- 建議控制措施列表欄位勾選已建置,卻無相應之佐證資料
- 盤點表與評估表個資檔案筆數不同
- 評估表個資分類選取錯誤

注意事項

- 個資盤點有關保存年限參照問題?
  依序為法律法規、主管機關規定、學校規定、自訂合理理由
- 風險評鑑問題請詢問資訊處服務台:分機2468

個資檔案安全管理

- 選擇密碼原則：
  - 密碼長度不得少於6個字元
    複雜度至少應包括英文大寫、英文小寫、數字、符號其中兩項
  - 至少每90天宜變更一次
  - 不得與前 1 次之密碼重複
- 啟動密碼式電腦螢幕保護程式。
- 存放公用資料夾及公用電腦之個人資料檔案應依保留時間刪除。

測驗

謝謝大家~