個資清冊與威脅弱點評估完成後，風險處理計畫說明

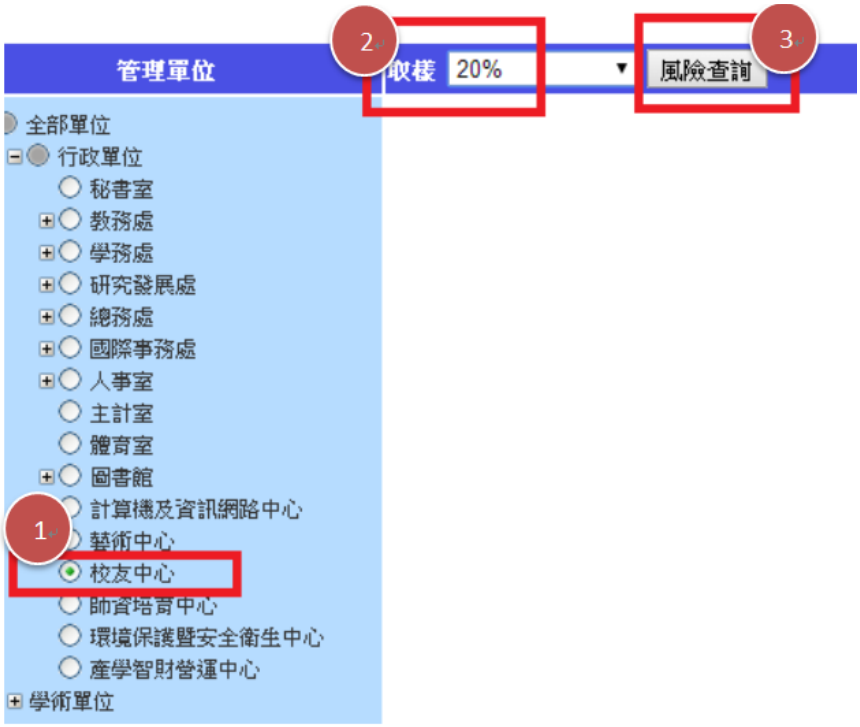
作業開始前小叮嚀：請先確認個資盤點與威脅弱點評估作業已經完成，否則若之後修改盤點或威脅弱點評估會造成轉出之計畫表不一致！

【1 登入】登入帳號：員工編號，共 7 碼

若未登入帳號密碼，無法進行風險值篩選與風險處理計畫作業。

【1 登入】
【2 進入衝擊分析及風險評鑑-風險值篩選】
【3 進行風險值篩選】
【4 風險值設定 20%篩選結果】
【5 匯出單位計畫表和彙整表】
【6 將系統上計畫表轉換為 Excel 檔案格式】
【7 將風險處理計畫 EXCEL 檔案完成】
【8 將風險處理計畫 EXCEL 列印下來交由單位主管簽核】

【2 進入衝擊分析及風險評鑑-風險值篩選】登入帳號後，點選此選項(紅框)進入風險值篩選作業



【3 進行風險值篩選】①先選單位　②取樣[20%] ③點選[風險查詢]

【4 風險值設定 20%篩選結果】

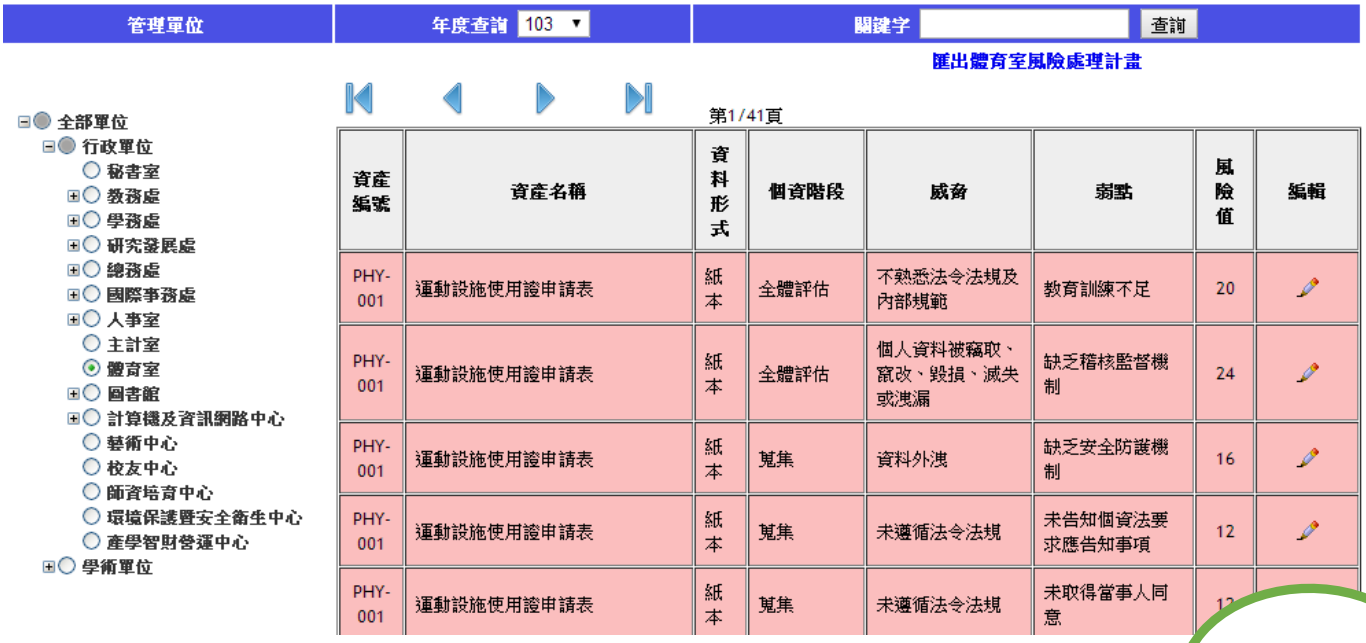
紅框部分，為篩選出的相關數值

黃框部分，為篩選出的結果

【5 匯出單位計畫表和彙整表】

點選畫面右上角「匯出 XX 單位計畫表和彙整表」

個資檔案風險處理計畫



匯出完成如上圖 上述為單位的風險處理計畫

請點選

個資檔案風險處理計畫

【6 將系統上計畫表轉換為 Excel 檔案格式】

匯出完成後請在點選 右上方 「匯出 **XX** 風險處理計畫」

即會進行將系統上資料轉換為 **EXCEL** 檔案

此時因系統上資料轉換為 **EXCEL** 檔案，需要一段時間，請耐心等候

個人資料檔案風險處理計畫

機密等級：□公開使用 ■內部使用 □內部限閱 □機密

文件編號：NCHU-PIMS-D-012　　版　　次：1.0

紀錄編號：　　填表日期：　　年　　月　　日

資產識別暨風險說明											風險處理措施		風險進度追蹤				
項次	單位	流程名稱	資產編號	個資檔案	個資型式	個資階段	威脅	弱點	風險說明	風險值	風險處理型式	改善活動/控制措施	負責人	預定完成日期	實際完成日期	覆核人員	風險處理
											□接受風險 □降低風險 □轉移風險 □避免風險						
											□接受風險 □降低風險 □轉移風險 □避免風險						
											□接受風險 □降低風險 □轉移風險 □避免風險						
											□接受風險 □降低風險 □轉移風險 □避免風險						
											□接受風險 □降低風險 □轉移風險 □避免風險						

四選一
1.個資外洩
2.違反個資法
3.違反BS10012標準規範
4.違反個資法及BS10012標準規

詳投影片第11頁

詳投影片第12頁~21頁

單位窗口

何時開始落實

實際落實日

主管、顧問等

已完成
OR
未完成

風險處理計畫表

- 風險說明欄位填寫(範例)
  - 個資外洩
  - 違反個資法
  - 違反BS10012標準規範
  - 違反個資法及BS10012標準規範

風險處理計畫表

- 風險處理型式
  - 接受風險
    - 符合組織的政策與風險接受準則，則知悉且客觀地接受風險。
  - 降低風險
    - 參考標準選擇適當之控制措施以降低風險。
    - 藉由加強各項作業之內控以降低風險發生之機會。
  - 轉移風險
    - 轉移相關之營運風險至他者，例如：承保商、供應商。
  - 避免風險
    - 修改作業方式或採用技術以避開風險。
    - 經由政策或標準以禁止從事高風險交易或活動。

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 不熟悉法令法規及內部規範、教育訓練不足：
    - 落實定期辦理個資教育訓練及法令、法規宣導。
  - 未保護儲存資料、未控管儲存媒體、儲存媒介內之資料沒有適當刪除就丟棄或重覆使用、儲存媒介之不當存取、 儲存媒介之不當存取：
    - 落實儲存媒介管理機制
    - 落實個人資料生命週期管理程序
    - 落實個人資料安全控管作業

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 未訂定保存期限、資料未依使用期限進行銷毀或刪除、資料銷毀處理程序不當或不足、缺乏回收控管機制：
    - 落實個人資料檔案保存期限，並辦理銷毀程序
    - 落實個人資料生命週期管理程序
    - 落實個人資料安全控管作業
  - 未提供履行當事人權利機制、未於法定期限內准駁
    - 依據履行當事人權利機制，落實於法定期限內准駁。

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 未經授權下處理資料、存取權限授與不當：
    - 落實權責單位進行權限控管並定期審查
    - 落實個人資料安全控管作業
  - 個人資料被竊取、竄改、毀損、滅失或洩漏、.缺乏安全防護機制、惡意行為：
    - 落實個資被竊取、洩漏、竄改於查明後告知之程序
    - 落實安全防護、環境控制、網路存取規劃機制
    - 落實個人資料生命週期管理程序
    - 落實個人資料安全控管作業
    - 落實定期辦理資訊安全教育訓練及宣導

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 缺乏實體保護、缺乏環境控制：
    - 落實安全防護、環境控制、網路存取規劃機制。
  - 設備損壞、操作錯誤
    - 落實因應設備損壞與有效維護之管理機制
    - 落實個人資料安全控管作業
  - 未主動或依當事人之請求更正或補充個人資料
    - 落實資料更新補充機制
  - 未告知個資法要求應告知事項
    - 落實個資法要求應告知事項、逾越特定目的與範圍之告知程序。

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 未取得當事人同意：
    - 落實取得當事人同意機制
  - 未於法定期限內准駁、未提供履行當事人權利機制：
    - 履行當事人權利機制，並落實於法定期限內准駁。
  - 未保護儲存資料：
    - 落實個人資料安全防護、環境控制、網路存取規劃機制。
    - 落實電腦與應用系統安全管控機制。

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 未訂定保存期限：
    - 依據個人資料檔案保存期限，落實辦理銷毀程序
    - 落實個人資料生命週期管理程序
    - 落實個人資料安全控管作業
  - 未提供當事人表示拒絕接受行銷之方式：
    - 落實拒絕接受行銷之機制
  - 未經授權下處理資料：
    - 權責單位進行權限控管並定期審查
    - 落實個人資料安全控管作業

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 委外利用資料、委外蒐集資料：
    - 落實委外廠商管理及監督機制。
    - 落實委外蒐集作業管理程序。
  - 個人資料被竊取、竄改、毀損、滅失或洩漏：
    - 落實個資被竊取、洩漏、竄改於查明後告知之程序
    - 落實安全防護、環境控制、網路存取規劃機制
    - 落實定期辦理資訊安全教育訓練及宣導
  - 個資被竊取、洩漏、竄改未於查明後告知
    - 落實個資被竊取、洩漏、竄改於查明後告知之程序

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 缺乏安全防護機制：
    - 落實安全防護機制(如：資料傳輸加密、存取權限管控)
  - 缺乏稽核監督機制：
    - 落實稽核監督之管理機制
    - 定期執行稽核查檢作業
  - 惡意或不當行為(外部傳送）：
    - 落實安全防護、環境控制、網路存取規劃機制。
    - 落實個人資料傳輸管理程序。

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 缺乏安全防護機制：
    - 落實安全防護機制(如：資料傳輸加密、存取權限管控)
  - 傳輸過程未有適當之加密或保護(資料外洩)：
    - 落實個人資料傳輸管理程序。
    - 落實電腦與應用系統安全管控機制。
  - 傳輸過程未有適當之保護(錯誤資訊)：
    - 落實個人資料傳輸管理程序。
    - 權責單位進行權限控管並定期審查。

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 資料外洩：
    - 落實個資被竊取、洩漏、竄改於查明後告知之程序
    - 落實安全防護、環境控制、網路存取規劃機制
    - 落實定期辦理資訊安全教育訓練及宣導
  - 蒐集特種資料：
    - 落實特種個資蒐集機制(如：告知事項、取得當事人書面同意)
  - 蒐集資訊缺乏正當合理之關聯：
    - 落實定期審查蒐集資訊缺乏正當合理關聯之機制。