致理科技大學

個人資料風險評估填寫說明

機密等級：■一般 □敏感 □機密

編號：P-3-01

版本：1.2

發行日期：106 年 6 月 15 日

文件制／修訂紀錄頁

版次	發行日期	修訂摘要	修訂者	文管人員
1.0	106.4.20	初次發行	呂瑞茹	呂瑞茹
1.1	106.5.19	修改影響及衝擊等級表之可識別性說明，「非常嚴重」新增文字「例如：身分證字號」	呂瑞茹	呂瑞茹
1.2	106.6.15	修改個人資料檔案的風險值的計算方式	林裕淇	呂瑞茹

目錄

壹、 評估項目說明：

個人資料檔案風險評估分別評估下列幾個項目

- 個人資料檔案價值
  為個人資料檔案所含包含之個人資料內容價值。
- 衝擊程度
  為當個人資料檔案發生外洩等事故時可能對各方面所產生的衝擊影響。
- 外洩可能性
  為該個人資料檔案發生如外洩等事故的可能性高低。

由個人資料價值、衝擊程度與發生的可能性等三個因素來決定個人資料檔案的風險值。

貳、 評估作業指引：

一、風險評估與分析

1. 個人資料風險評估由各單位依據實際狀況，對照「影響及衝擊等級表」及「風險發生可能性等級表」之內容，識別組織面臨內部弱點及外在威脅所產生之影響與衝擊程度，並將評估結果記錄於「個人資料檔案風險評估彙整表」。

2. 個資檔案影響及衝擊分析參照「影響及衝擊等級表」六個評估項目(構面)，應依各個人資料檔案於各評估項目之實際狀況，分別給予輕微(1)、嚴重(2)、非常嚴重(3)等三種不同之影響及衝擊值，由各評估構面中選擇衝擊等級最高的作為其衝擊程度(I)。「影響及衝擊等級表」之內容如下說明。

評估項目（構面）	影響及衝擊(I)等級表		
	輕微(1)	嚴重(2)	非常嚴重(3)
可識別性	個人資料查詢困難，耗費過鉅或耗時過久始能識別特定當事人者。	僅可以間接識別特定當事人者(**需要**與其他資料進行對照、組合、連結等，始能識別該特定的個人)	可以直接識別特定當事人者，例如：身分證字號(**不需要**與其他資料進行對照、組合、連結等，就能識別該特定的個人)
個資數量	200 筆以下	一般個資 201~20,000 筆 特種個資 201~2,000 筆	一般個資 20,001 筆以上 特種個資 2,001 筆以上
敏感程度	僅有識別資料 (未含其他個人活動、財務金融或特種個人資料)	除識別資料外，還含有個人活動資料或財務金融資料	含有特種個人資料 (病歷、醫療、基因、性生活、健康檢查、犯罪前科)

特定目的範圍內利用	僅於特定目的範圍內利用個資	有特定目的外利用個資，但符合例外條款	有特定目的外利用個資，但不符合例外條款
蒐集處理利用	無外部利用情形	無償委任關係外部利用(例：公務部門)	有償委任關係外部利用(例：廠商)
國際傳輸	無國際傳輸情形	主管機關未規定之國際傳輸	主管機關訂定規定之國際傳輸

3. 各單位應參照「風險發生可能性等級表」進行風險發生可能性之評估分析。風險發生之可能性，應依據各個人資料檔案之實際狀況，分別給予低(1)、中(2)、高(3)等三種不同之可能性等級值，由各評估構面中發生可能性等級最高的作為其風險發生可能性等級(P)。「風險發生可能性等級表」之內容如下說明。

評估項目（構面）	風險發生可能性(P)等級表		
	高(3)	中(2)	低(1)
教育訓練	業務相關人員 60%以上(含)未接受相關教育訓練。	部分業務相關人員(10%以上(不含)、60%以下(不含)曾接受相關教育訓練。	業務相關人員 90%以上(含)曾接受完整教育訓練。
作業管理規定	個人資料檔案之處理流程，未訂有書面標準作業程序，僅依經驗共識執行。	該個人資料檔案之處理流程，訂有書面標準作業程序，僅依經驗執行，並未確實落實。	已建立並實施個人資料保護相關作業程序規範，並確實落實執行。
內部監督稽核或監督管理	單位未建立內部稽核或未執行監督管理機制。	單位已建立內部稽核或監督管理機制，但單位未落實監督管理作業與持續改善。	單位已建立內部稽核或監督管理機制，已定期執行稽核與監督管理作業，並確實執行持續改善。

個人資料檔案不當存取	個人資料檔案過去三年內曾發生二次(含)以上外洩或不當存取情形。	個人資料檔案過去三年內曾發生一次外洩或不當存取情形。	個人資料檔案過去三年內未曾發生過外洩或不當存取情形。

二、 風險值計算

由各單位識別出個人資料檔案影響/衝擊程度(I)及風險發生之可能性(P)，並將此 2 項評估值進行相乘，即求出該個人資料檔案之風險值。

風險值(R) =影響/衝擊程度(I) ×可能性(P)。

三、 風險分布矩陣

將經由風險值計算公式所得之風險值，對應至「風險分布矩陣」以判斷風險值之分布情況。

風險分布矩陣			
	發生機率		
影響/衝擊程度	幾乎不可能(1)	有可能(2)	幾乎確定(3)
輕微(1)	1(低度)	2(低度)	3(中度)
嚴重(2)	2(低度)	4(中度)	6(高度)
非常嚴重(3)	3(中度)	6(高度)	9(極高度)

四、 個資風險等級判定

可接受風險值：以下列出可接受及不可接受之風險等級，作為本校各單位後續風險處理之依據。

風險值(R)	風險等級	風險判別與處理	
1 或 2	1	可接受風險	接受
3 或 4	2	可接受風險	持續監視
6 或 9	3	不可接受風險	立即控制

五、 撰寫風險評估報告

（一）各單位完成個人資料檔案風險評估後，由各單位承辦人員整併「個人資料檔案風險評估彙整表」，陳單位主管審核後由各單位進行存檔備查。

（二） 各單位完成「個人資料檔案風險評估彙整表」後，由各單承辦人員負責撰寫各單位之「個人資料風險評估報告」，並由單位主管提出可接受之風險值建議。

六、 個人資料檔案風險管理

（一）決定可接受之風險值：可接受風險值納入程序書加以律定，得考量各單位作業環境及安全控管現況作適當調整。

（二）個資檔案風險處理作業

1. 依個人資料檔案風險評估結果及可接受風險值之決議，針對高於可接受風險值之檔案應由各單位業務承辦人員對需降低風險值之個人資料檔案，擬訂「個資風險處理計畫」，以期將風險降至可接受等級。
2. 風險處理計畫之風險處理措施，應根據「個人資料保護法」及參考國際個人資料保護管理標準，對各項個人資料保護之安全要求目標，擬訂適當之處理措施及相關執行資源。
3. 風險處理計畫所採行之控制措施，於實施時應建立相對應之有效性量測，以反映出控制措施實施狀況及成效，以利管理階層及相關人員定期或不定期審視，以達降低風險之目標。
4. 「個資風險處理計畫」應經審查後執行，並列入追蹤管理。
5. 風險處理計畫之風險處理措施及說明、改善活動與其所需資源、預訂完成日期等規劃項目，應詳實記錄於個人資料檔案風險處理計畫表之對應欄位，並納入管審會議管制。

（三）風險處理計畫執行成效暨殘餘風險處理

1. 風險處理計畫於預訂完成日期結束後，須由各單位執行風險再評鑑，以確認風險處理計畫執行達到風險減緩預期目標，並將風險再評鑑之結果填寫於「個人資料檔案風險評估彙整表」，提報管審會議審查。
2. 實施控制的風險，若處理結果已降至風險可接受等級之下，應於管理審查會議中提出討論，決定是否列入下次風險評鑑審查事項。
3. 若處理後之風險值如無法降至風險可接受等級之下，應於管審會議中

提出討論，並決定是否接受此風險或是重新擬定風險處理計畫，採行其他可行之控制措施。

參、 使用表單：

一、 個人資料檔案風險評估彙整表。(P-2-05-01)

二、 個人資料風險評估報告。(P-2-05-02)

三、 個人資料風險處理計畫。(P-2-05-03)