



文件編號	PIMS-P-016	文件名稱	個人資料風險評鑑與處理管理程序		
機密等級	內部使用	版 次	A	頁次	1 / 10

管理系統文件

文件類別	第二階文件	
文件編號	PIMS-P-016	
文件名稱	個人資料風險評鑑與處理管理程序	
發行單位	文件管制中心	
發行日期	103年12月01日	
版 次	A	
訂修廢單位	審 查	核 准
個資保護執行 小組		

(原版簽名頁保存於文件管制中心)



文件編號	PIMS-P-016	文件名稱	個人資料風險評鑑與處理管理程序		
機密等級	內部使用	版 次	A	頁次	3 / 10

1. 目的

中州科技大學（以下簡稱為本校）為建立個人資料風險評鑑與處理作業有一明確之規範，提供共同遵行之風險評估標準，採取適當之對策或控制措施，以有效降低個人資料遭受損害的風險，特訂定本程序。

2. 適用範圍

凡本校各單位依業務流程導向進行個人資料風險評估作業之管理，均適用本程序。

3. 參考文件

- 3.1. 中華民國個人資料保護法。
- 3.2. 中華民國個人資料保護法施行細則。
- 3.3. PIMS-M-001 個人資料保護管理政策。

4. 名詞定義

- 4.1. 可接受風險值
個人資料資產之最低風險容忍度。
- 4.2. 殘餘風險 (RESIDUAL RISK)
在採用相關控制措施之後剩餘的風險。
- 4.3. 威脅 (THREAT)
可能對個人資料資產或組織造成傷害之意外事件。
- 4.4. 弱點 (VULNERABILITY)
因個人資料資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。
- 4.5. 隱私衝擊分析 (PRIVACY IMPACT ASSESSMENT, PIA)
用以識別各個人資料檔案其隱私或個人資料於收集、使用和揭露過程中可能產生之衝擊程度。
- 4.6. 風險 (RISK)
可能對團體或組織的個人資料資產發生損失或傷害的潛在威脅，通常



文件編號	PIMS-P-016	文件名稱	個人資料風險評鑑與處理管理程序		
機密等級	內部使用	版 次	A	頁次	4 / 10

用產生之影響來衡量。

4.7. 個人資料

泛指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動等。

5. 權責

5.1. 各單位個人資料代表

負責彙整單位內個人資料風險評鑑及處理作業，交由單位權責主管審核及確認。

5.2. 個資保護執行小組

5.2.1. 規劃制定衝擊等級、風險類型與風險等級之內容及評鑑方法。

5.2.2. 訂定組織可接受的風險等級。

5.2.3. 負責監督及管理各單位個人資料風險評鑑及處理作業。

5.3. 個人資料管理代表

審核各單位個人資料風險評鑑及處理作業。



文件編號	PIMS-P-016	文件名稱	個人資料風險評鑑與處理管理程序		
機密等級	內部使用	版次	A	頁次	5 / 10

6. 作業內容

6.1. 個人資料檔案風險評鑑與管理作業流程

作業流程	權責單位	相關文件
<div style="border: 1px solid black; border-radius: 15px; padding: 5px; display: inline-block;">鑑別個資檔案</div>	各單位個人資料代表	個資項目盤點表
↓		
<div style="border: 1px solid black; padding: 5px; display: inline-block;">鑑別個資檔案風險</div>	各單位個人資料代表	個資檔案風險評鑑彙整表
↓		
<div style="border: 1px solid black; padding: 5px; display: inline-block;">撰寫風險評估報告</div>	各單位個人資料代表	個資檔案風險評估彙整表 個資檔案風險評估報告
↓		
<div style="border: 1px solid black; width: 50px; height: 20px; margin: 0 auto; transform: rotate(45deg);"></div> 確認核估結果	個人資料管理代表	個資檔案風險評鑑報告
Yes ↓ No		
<div style="border: 1px solid black; padding: 5px; display: inline-block;">個資風險處理</div>	各單位個人資料代表	個人資料保護管理執行小組 個資檔案風險處理計畫
↓		
<div style="border: 1px solid black; width: 50px; height: 20px; margin: 0 auto; transform: rotate(45deg);"></div> 確認處理結果	個人資料管理代表	個人資料保護管理執行小組 個資檔案風險處理計畫
Yes ↓ No		
<div style="border: 1px solid black; border-radius: 15px; padding: 5px; display: inline-block;">紀錄保存</div>	各單位個人資料代表	



文件編號	PIMS-P-016	文件名稱	個人資料風險評鑑與處理管理程序		
機密等級	內部使用	版次	A	頁次	6 / 10

6.2. 鑑別個人資料檔案

本校個人資料及個人資料檔案之鑑別與盤點作業，請依據「PIMS-P-015 個人資料盤點作業管理程序」之相關規定辦理。

6.3. 鑑別個人資料檔案風險

6.3.1. 風險評估執行時機

個人資料風險評估作業應於每年辦理個人資料內部稽核活動前執行，各單位個人資料代表可視實際狀況，決定執行之時機與範圍。除每年定期執行一次外，亦應於下列情形發生時，針對變動範圍內的作業程序與個人資料檔案進行風險評鑑：

- 6.3.1.1. 本校營運組織發生變更。
- 6.3.1.2. 作業環境、作業流程或系統重大變更或異動。
- 6.3.1.3. 新增或變更個人資料檔案。
- 6.3.1.4. 發生重大個人資料外洩事件。

6.3.2. 風險評估與分析

- 6.3.2.1. 個人資料檔案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「PIMS-P-016-01 個資檔案風險評估彙整表」。
- 6.3.2.2. 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。「影響及衝擊等級表」之內容如下說明。

評估項目 (構面)	影響及衝擊等級表(I)		
	輕微(1)	嚴重(2)	非常嚴重(3)
可識別性	個資查詢困難，耗費過鉅或耗時過久始能識別特定當事人者	可以間接識別特定當事人者	可以直接識別特定當事人者



文件編號	PIMS-P-016	文件名稱	個人資料風險評鑑與處理管理程序		
機密等級	內部使用	版次	A	頁次	7 / 10

個資數量	20 筆以下 (團體訴訟不成立)	一般個資 21~10,000 筆 特種個資 21~1,000 筆	一般個資 10,001 筆以上 特種個資 1,001 筆以上
敏感程度	僅有識別資料，未含其他個人活動資料	含有個人活動資料或財務金融資料	含有特種個人資料
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
外部利用	無外部利用情形	無償委任關係外部利用	有償委任關係外部利用
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

註記：評估項目參考 [NIST SP800-122](#) 選定，等級判定依據個資法之相關要求訂定，依據以上項目分項判定，最後依據最高衝擊原則，判定衝擊程度等級。

6.3.2.3. 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。「風險發生可能性等級表」之內容如下說明。

等級	可能性	發生機率	描述
3(高)	幾乎確定	61-100%	在大部分的情況下會發生
2(中)	有可能	41-60%	有些情況下會發生
1(低)	幾乎不可能	0-40%	只會在特殊的情況下發生

6.3.3. 風險值計算

6.3.3.1. 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。

6.3.3.2. 風險值(R) = 影響/衝擊程度(I) × 可能性(P)。

6.3.4. 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。



文件編號	PIMS-P-016	文件名稱	個人資料風險評鑑與處理管理程序		
機密等級	內部使用	版 次	A	頁次	8 / 10

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

6.3.5. 個資風險等級判定

6.3.5.1. 決定可接受風險值

6.3.5.1.1. 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

6.3.5.1.2. 各單位個人資料風險評估可接受之風險等級，每年需檢討並經「個人資料保護管理執行小組」開會決議並記載於會議紀錄中。

6.4. 撰寫風險評估報告

6.4.1. 各單位完成個人資料檔案風險評估後，由各單位個人資料代表整併「PIMS-P-016-01 個人資料檔案風險評估彙整表」，陳單位主管審核後，交由個資保護執行小組進行彙整。

6.4.2. 個資保護執行小組依據各單位「PIMS-P-016-01 個資檔案風險評估彙整表」之內容，撰寫本校「PIMS-P-016-02 個資檔案風險評估報



文件編號	PIMS-P-016	文件名稱	個人資料風險評鑑與處理管理程序		
機密等級	內部使用	版 次	A	頁次	9 / 10

告」，並提出可接受之風險值建議。

6.5. 個人資料檔案風險管理

6.5.1. 決定可接受之風險值

本校個人資料檔案風險評估之可接受風險值，需經「個人資料保護管理執行小組」開會決議，並記載於會議紀錄中。

6.5.1.1. 「個人資料保護管理執行小組」每年召開會議檢討可接受之風險值。可接受風險值得考量各單位作業環境及安全控管現況作適當調整。

6.5.2. 個資檔案風險處理作業

6.5.2.1. 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之檔案應由各單位個人資料代表對需降低風險值之個人資料檔案，擬訂「PIMS-P-016-03 個資檔案風險處理計畫」，以期將風險降至可接受等級。

6.5.2.2. 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。

6.5.2.3. 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。

6.5.2.4. 「PIMS-P-016-03 個資檔案風險處理計畫」應提報「個人資料保護管理執行小組」審查後執行，並列入追蹤管理。

6.5.2.5. 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，並於預訂完成日期結束後，提報「個人資料保護管理執行小組」。

6.5.3. 風險處理計畫執行成效暨殘餘風險處理

6.5.3.1. 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



文件編號	PIMS-P-016	文件名稱	個人資料風險評鑑與處理管理程序		
機密等級	內部使用	版 次	A	頁次	10 / 10

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「PIMS-P-016-01 個資檔案風險評估彙整表」，提報管審會議審查。

6.5.3.2. 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。

6.5.3.3. 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。

7. 相關表單

7.1. PIMS-P-016-01 個資檔案風險評估彙整表。

7.2. PIMS-P-016-02 個資檔案風險評估報告。

7.3. PIMS-P-016-03 個資檔案風險處理計畫。