國立中興大學

個人資料檔案風險評鑑與管理程序書

機密等級：內部使用

文件編號：**NCHU-PIMS-B-003**

版　　次：**1.3**

發行日期：**106.10.02**

本文件歷次變更紀錄：

版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	101.10.22	N/A	資安暨個資保護執行小組	初版發行
1.1	102.03.20	P.6	資安暨個資保護推動委員會	威脅暨弱點分析評鑑構面異動
1.2	104.06.11	P.6	資安暨個資保護推動委員會	威脅暨弱點分析評鑑構面異動
1.3	106.10.02	P.6~ P.9	資安暨個資保護推動委員會	1. 新增「風險擁有者」定義、高風險個資之管制措施。 2. 修訂作業內容，符合實際作業流程。

目　　錄

壹、目的

為建立國立中興大學（以下簡稱本校）個人資料檔案風險評鑑與管理規範，提供共同遵行之風險評鑑標準，採取適當之對策或控制措施，以有效降低個人資料檔案遭受損害的風險，特訂定本程序書。

貳、適用範圍

一、本程序書適用範圍為本校業務相關作業流程產生之個人資料檔案風險評鑑事宜。

二、以個人資料檔案為風險評鑑標的。

三、個人資料管理制度控制措施有效性量測。

參、權責

一、 召集人/執行秘書

(一) 視實際狀況決定個人資料檔案風險評鑑之時機與範圍。

(二) 監督個人資料檔案風險評鑑之執行。

(三) 個人資料檔案風險評鑑結果之審查及確認。

(四) 覆核個人資料檔案風險評鑑報告。

(五) 有效性量測之審查及確認。

二、 各權責單位主管（風險擁有者）

(一) 負責所屬單位業務範圍之風險評鑑結果審核作業。

(二) 個人資料檔案風險處理計畫之審查，如當風險值計算完成後，進行風險管理工作，其責任為資源分配、剩餘風險等級之接受等。

三、 資安暨個資保護執行小組

(一) 依據本程序書執行個人資料檔案之風險評鑑與處理。

(二) 指派專人彙總「個人資料檔案威脅及弱點評估表」。

(三) 依據個人資料風險評鑑結果建議可接受風險等級。

(四) 指派專人彙總「個人資料檔案風險處理計畫」並提報審核。

(五) 個人資料檔案清冊之管理與維護。

(六) 擬定、執行個人資料檔案風險處理計畫，並評估風險處理計畫執行成效。

(七) 擬定、執行有效性量測作業。

(八) 實施個人資料檔案風險再評鑑作業。

肆、定義

一、可接受風險值

個資資產之最低風險容忍度。

二、殘餘風險 (RESIDUAL RISK)

在採用相關控制措施之後剩餘的風險。

三、威脅 (THREAT)

可能對個資資產或組織造成傷害之意外事件。

四、弱點 (VULNERABILITY)

因個資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。

五、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。

六、風險 (RISK)

可能對團體或組織的個資資產發生損失或傷害的潛在威脅，通常用產生之影響來衡量。

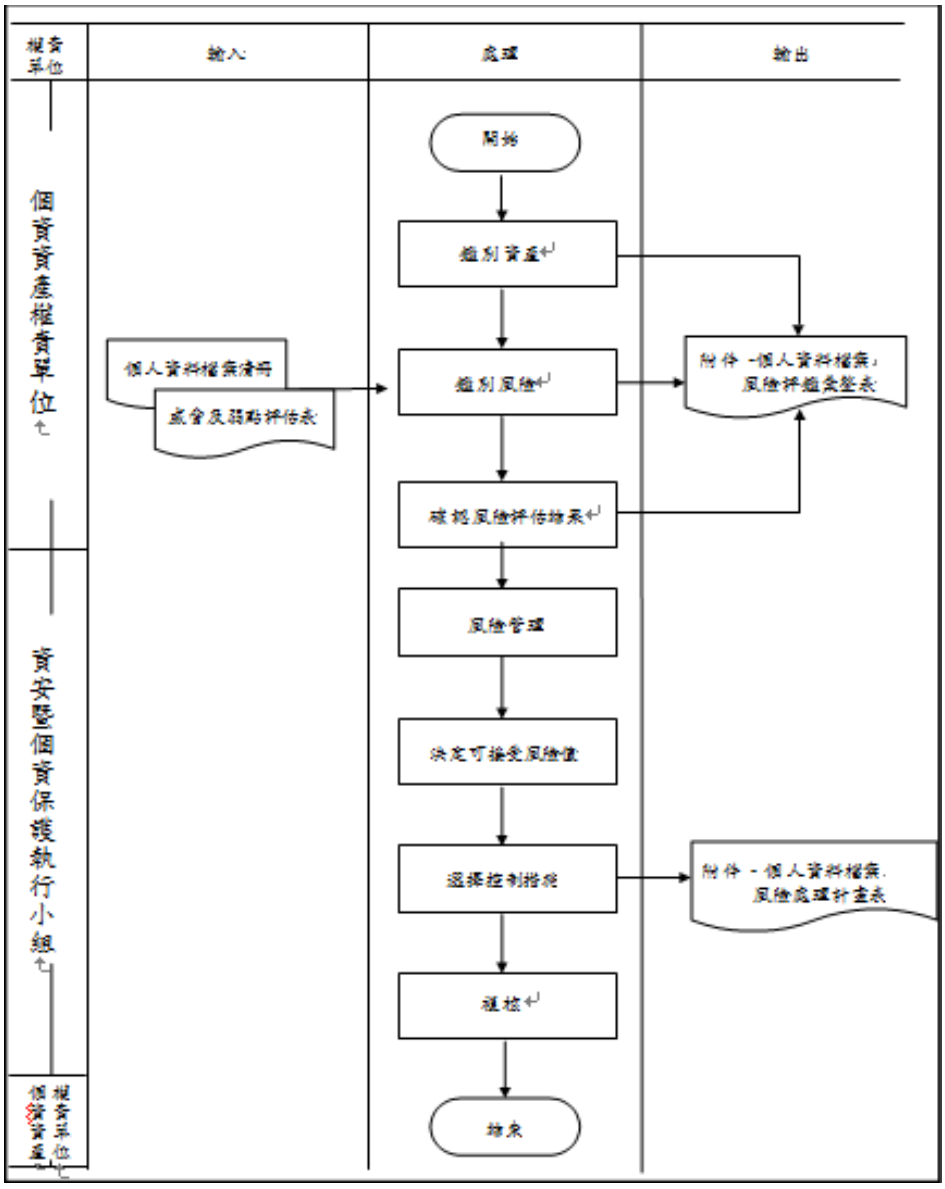
七、個人資料

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。

伍、作業內容

一、個人資料保護管理制度個人資料風險管理作業流程圖



二、個人資料資產分類

本校個人資料資產分為電子與紙本兩類別，其分類說明如下：

(一) 電子資料(DATA；DA)：係指儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊，包含公文、報表、表單、計畫書、合約、外來文件及資料庫資料等電子檔案。

(二) 紙本資料(DOCUMENT；DC)：係指以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫、文件等紙本資料。

三、個人資料檔案鑑別

(一) 資安暨個資保護執行小組(各單位聯絡窗口)應進行組織業務個資盤點作業，並視實際狀況進行內容調整。

(二) 依據作業流程分析結果，執行個人資料檔案鑑別作業，並建立「個人資料檔案清冊」。

(三) 應針對個資法第六條所限定蒐集之個人資料視為高風險個人資料或其他具敏感個人資料，依據【個人資料文件管理程序書】對應之文件等級進行標示與相關管制措施。

(四) 本校除每年執行一次個人資料檔案鑑別作業外，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個人資料檔案鑑別作業：

1. 營運組織變更。
2. 作業流程改變。

四、個人資料資產之群組歸納原則

依據各單位識別出之個資資產進行分類，再從分類中群組化，以避免遺漏重要資產，群組歸納原則如下：

(一) 個資資產價值相同。

(二) 個資資產性質相同。

(三) 個資欄位要相同且資產數量較多。

五、個資隱私衝擊分析

(一) 資安暨個資保護執行小組針對「個人資料檔案清冊」內容，依據 「個資衝擊影響程度表」定期進行個資資產之衝擊影響程度分析，衝擊影響程度說明如下：

個資衝擊影響程度表

衝擊 影響程度	資產價值 (衝擊值)	個人資料範圍
極高	4	自然人之姓名或國民身分證統一編號 (或護照號碼) 及特種個人資料。
高度	3	1. 含自然人之姓名**及**國民身分證統一編號（或護照號碼），但不含特種個人資料。 2. 含自然人之姓名或國民身分證統一編號(或護照號碼)及財務情況（如：薪資、局帳號），但不含特種個人資料。
中度	2	1. 含自然人之姓名或國民身分證統一編號(或護照號碼)，但不包含特種資料。 2. 含自然人之姓名**及**員工編號（或學號），但不含特種個人資料。
一般	1	不含自然人之姓名及國民身分證統一編號(或護照號碼)。

(二) 個人資料檔案資產價值（衝擊值）評估

個人資料檔案之資產價值（衝擊值）依據每個個資檔案內容所涵蓋之個人資料範圍，分別給予一般(1)、中度(2)、高度(3)與極高(4)等四個不同之資產價值（衝擊值）。

六、個人資料檔案風險評鑑

(一) 鑑別個人資料檔案資產價值，如伍、五說明。

(二) 個人資料檔案風險評鑑作業應於每年內部稽核活動前執行，資安暨個資保護執行小組可視實際狀況，決定執行之時機與範圍。除每年執行一次外，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：

1. 營運組織變更。
2. 作業流程改變。
3. 新增或變更個人資料檔案。

4. 發生重大個資外洩事件。

(三) 威脅及弱點影響分析

個人資料檔案之威脅及弱點評估依據「個人資料檔案威脅暨弱點分析評分構面表」於「個人資料檔案威脅及弱點評估表」進行構面之風險分析，本表係參酌「個人資料保護法」內容與控管設計，以利評估組織在面臨個資風險時可能產生之影響程度。

1. 各單位須針對各項個人資料檔案之使用及控管狀況，依據「個人資料檔案威脅暨弱點分析評分構面表」之各構面，識別其面臨組織內部弱點及外在威脅所產生之影響程度。

2. 本校個人資料檔案威脅及弱點分析結果應彙整於個人資料檔案威脅及弱點評估表。

(四) 威脅及弱點評估加權調整

當評估構面因子時，本校可依據實際需求考量（如單位文化、營運風險或環境變更等），調整每個構面對組織之影響權重，以凸顯組織所面臨個人資料檔案於蒐集、處理、利用、保存、銷毀及傳輸等過程因外洩、竄改或損毀所產生之影響。

(五) 個人資料檔案風險值計算

1. 評估個人資料檔案威脅及弱點對構面因子所產生之影響，計算出風險值。

2. **風險值** = 資產價值（衝擊值）×（構面值 1 × 權重 + 構面值 2 × 權重 + 構面值 3 × 權重 + 構面值 4 × 權重）。

(六) 風險評鑑報告產出

依據個人資料檔案風險評鑑結果撰寫個人資料檔案風險評鑑報告，並由資安暨個資保護執行小組提出可接受之風險等級建議。

七、個人資料檔案風險管理

(一) 決定可接受風險值

1. 本校個人資料檔案風險評鑑之可接受風險值，需經「資訊安全暨個人資料保護推動委員會」開會決議，並記載於會議紀

錄中。

2. 除決定可接受風險值外，亦可訂定風險處理之補償條件，篩選出可接受風險值以下，但仍須進行風險處理之個人資料檔案項目。

3. 「資訊安全暨個人資料保護推動委員會」每年召開會議檢討可接受風險值。可接受風險值得考量本校作業環境及安全控管現況作適當調整。

(二) 個人資料檔案風險處理計畫作業

1. 依個人資料檔案風險評鑑結果及可接受風險值之決議，由各風險項目負責人針對需降低風險值之個人資料檔案，並擬訂「個人資料檔案風險處理計畫」，以期將風險降至可接受程度。

2. 個人資料檔案風險處理計畫之風險處理措施，應根據「個人資料保護法」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之資訊。

3. 個人資料檔案風險處理計畫應由各權責單位主管（風險擁有者）審查，並列入追蹤管理。

4. 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記錄於「個人資料檔案風險處理計畫表」之「風險處理進度」欄。

5. 個人資料檔案風險處理計畫若為長期之專案計畫，則應於執行前進行風險評估，確認其預期效益可達到風險處理之目標，並於專案各階段驗收後，提報「資訊安全暨個人資料保護推動委員會」討論執行之成效與進度。

(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，須由資安暨個資保護執行小組(各單位聯絡窗口)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效益，並將風險再評鑑之結果填寫於個人資料檔案風險評鑑彙整表。

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. 若處理後之風險值無法降至風險可接受等級之下，應於管理審查會議中提出討論，決定是否接受此風險或增加其他控制。

八、個人資料檔案威脅及弱點評估審查

(一) 監控

1. 控制措施的實施應視需要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。

2. 任何可能造成當事人損失或(及)困擾之個人資料處理流程，應於「資訊安全暨個人資料保護推動委員會」中向個資召集人與個人資料風險擁有者進行陳報。

(二) 持續改善

為維持本風險評鑑方法之有效性，「資訊安全暨個人資料保護推動委員會」應：

1. 每年檢討可接受風險值與「個人資料檔案威脅及弱點評估表」之威脅及弱點項目。

2. 將發生個資事故或遭遇個資訴訟判決相關資訊，納入「個人資料檔案威脅及弱點評估表」威脅及弱點項目之檢討。

九、風險評鑑頻率

(一) 每年應至少執行 1 次風險評鑑。

(二) 當作業環境、作業流程變更或系統重大異動時，應不定期執行風險評鑑。

陸、參考文件

一、個人資料保護法。

二、個人資料文件管理程序書。

柒、相關表單

一、個人資料檔案清冊。

二、個人資料檔案威脅暨弱點分析評分構面表。

三、個人資料檔案威脅及弱點評估表。

四、個人資料檔案風險評鑑彙整表。

五、個人資料檔案風險處理計畫。