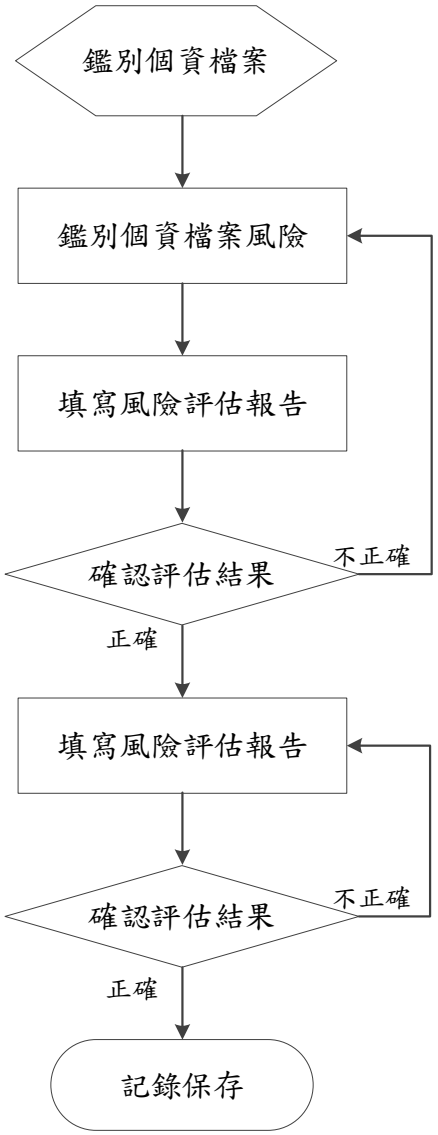
<table>
<tr><td colspan="5">南 華 大 學</td></tr>
<tr><td>文件編號</td><td>1500-3-213</td><td>文件名稱</td><td>修訂日期</td><td>109 年 03 月 30 日</td></tr>
<tr><td rowspan="2">制定單位</td><td>資訊中心</td><td rowspan="2">個人資料風險評估
標準作業流程</td><td rowspan="2">頁數</td><td>第1頁</td></tr>
<tr><td>系統發展組</td><td>共4頁</td></tr>
</table>

一、資訊處理事項：

◎個人資料風險評估作業

1. 流程圖：

流程	權責	表單
	各單位個人資料保護專責人員 各單位個人資料保護專責人員 各單位個人資料保護專責人員 單位主管 各單位個人資料保護專責人員 權責單位主管 各單位個人資料保護專責人員	個資項目盤點表 個資檔案風險評估彙整表 個資檔案風險評估彙整表 個資檔案風險評估報告 個資檔案風險評估報告 個資檔案風險處理計畫 個資檔案風險處理計畫

2. 作業程序：

2.1. 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「NHU-PIMS-2-003個人資料盤點作業管理程序」之相關規定辦理。

2.2. 鑑別個人資料檔案風險

2.2.1. 風險評估執行時機

2.2.1.1. 每年執行一次個人資料風險評估作業。

2.2.1.2. 本校營運組織發生變更。

2.2.1.3. 作業環境、作業流程或系統重大變更或異動。

2.2.1.4. 新增或變更個人資料檔案。

2.2.1.5. 發生重大個人資料外洩事件。

2.2.2. 風險評估與分析

2.2.2.1. 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「NHU-PIMS-2-004-01個資檔案風險評估彙整表」。

2.2.2.2. 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。

2.2.2.3. 評估項目(構面)將依相關規定變動進行調整。

2.2.2.4. 「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(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	20 筆以下 (團體訴訟不成立)	一般個資 21~20,000 筆 特種個資 21~2,000 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 (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
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

2.2.2.5. 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)	有可能發生	61-100%	平均每年都可能發生一次以上
2(中)	發生頻率低	41-60%	平均每年發生的次數不到一次
1(低)	不太可能發生	0-40%	沒有發生過，但是有發生的可能

2.2.3. 風險值計算

2.2.3.1. 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。

2.2.3.2. 風險值(R) =影響/衝擊程度(I) ×可能性(P)。

2.2.4. 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。

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)
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)

2.3. 撰寫風險評估報告

2.3.1. 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「NHU-PIMS-2-004-01個資料檔案風險評估彙整表」。

2.3.2. 單位完成「NHU-PIMS-2-004-01個資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「NHU-PIMS-2-004-02個資風險評估報告」

2.4. 確認評估結果

各單位個人資料保護專責人員風險評估作業完成時，交由權責單位主管審核及確認。

2.5. 記錄保存

各單位個人資料保護專責人員應將「NHU-PIMS-2-004-01個資檔案風險評估彙整表、

NHU-PIMS-2-004-02個資風險評估報告、NHU-PIMS-2-004-03個資風險處理計畫」自行進行存檔備查。

3. 控制重點：

3.1. 是否每年執行一次個人資料風險評估作業。

3.2. 是否於營運組織發生變更時，執行個人資料風險評估作業。

3.3. 是否於作業環境、作業流程或系統重大變更或異動時，執行個人資料風險評估作業。

3.4. 是否於新增或變更個人資料檔案時，執行個人資料風險評估作業。

3.5. 是否於發生重大個人資料外洩事件時，執行個人資料風險評估作業。

4. 使用表單：

4.1. NHU-PIMS-2-004-01個資檔案風險評估彙整表

4.2. NHU-PIMS-2-004-02個資風險評估報告

4.3. NHU-PIMS-2-004-03個資風險處理計畫

5. 依據及相關文件：

5.1. 依據南華大學PIMS程序書「NHU-PIMS-2-004個人資料風險評鑑與處理管理程序書」之辦法

6. 修訂紀錄：

序號	修訂內容	修訂日期
1	新訂文件	107/12/19
2	依據因應新版教育體系資通安全暨個人資料管理規範(草案)所改版之程序書，修改相關文字及使用表單。	109/02/20
3	1. 文件提及業務權責主管部分，統一使用「權責單位主管」名稱。 2. 將決策圖路徑修改為「正確」與「不正確」。	109/03/30