國立宜蘭大學

個人資料風險評鑑與管理程序書

機密等級：限閱

文件編號：NIU-PIMS-B-003

版　　次：1.1

發行日期：110 年 12 月 01 日

修 訂 紀 錄				
版次	**修訂日期**	**修訂頁次**	**修訂者**	**修訂內容摘要**
1.0	107 年 10 月 31 日		游佳欣	初版
1.1	110 年 12 月 01 日	8、9	游育豪	增加「適用性聲明書」

目錄

個人資料風險評鑑與管理程序書					
文件編號	NIU-PIMS-B-003	機密等級	限閱	版次	1.1

1 目的

為建立國立宜蘭大學（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。

2 參考依據

2.1 「個人資料保護法」。

2.2 「教育體系資通安全暨個人資料管理規範」。

3 適用範圍

3.1 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。

3.2 以個人資料檔案為風險評鑑標的。

3.3 個人資料管理制度控制措施有效性量測。

4 權責

4.1 召集人／執行秘書

4.1.1 視實際狀況決定個人資料檔案風險評鑑之時機與範圍。

4.1.2 監督個人資料檔案風險評鑑之執行。

4.1.3 個人資料檔案風險評鑑結果之審查及確認。

4.1.4 覆核個人資料檔案風險評鑑報告。

4.1.5 個人資料檔案風險處理計畫之審查。

4.1.6 有效性量測之審查及確認。

4.2 各權責單位主管（風險擁有者）

4.2.1 負責所屬單位業務範圍之風險評鑑結果核准與確認作業。

4.2.2 制訂風險處理計畫，並取得風險擁有者對風險處理計畫之核准，以及對剩餘風險之接受。

4.3 個資保護執行小組

4.3.1 依據本程序書執行權責單位個人資料檔案之風險評鑑與處理。

4.3.2 指派專人彙總權責單位「國立宜蘭大學個人資料檔案風險處理計畫」（NIU-PIMS-D-009）並提報審核。

4.3.3 權責單位個人資料檔案清冊之管理與維護。

4.3.4 擬定、執行權責單位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。

4.3.5 擬定、執行權責單位有效性量測作業。

4.3.6 分案及管制相關權責單位執行風險處理計畫。

5 定義

5.1 可接受風險值

個人資料資產之最低風險容忍度。

5.2 殘餘風險（RESIDUAL RISK）

在採用相關控制措施之後剩餘的風險。

5.3 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。

5.4 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，通常用產生之影響來衡量。

5.5 風險擁有者（Risk Owner）

權責單位內針對各項個人資料資產流程風險管理具備核准與確認者，由各權責單位主管擔任。

5.6 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、社會活動及其他得以直接或間接方式識別該個人資料。

6 作業說明

6.1 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：

6.1.1 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。

6.1.2 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。

6.2 個人資料檔案鑑別

6.2.1 個資保護執行小組（各單位個資保護聯絡窗口）應協助進行組織業務個資盤點作業，並視實際狀況進行內容調整。

6.2.2 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「國立宜蘭大學個人資料檔案清冊」(NIU-PIMS-D-007)。

6.2.3 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。

6.2.4 營運組織變更。

6.2.5 作業流程改變。

6.3 個人資料資產之群組歸納原則

依據各單位識別出之個人資料資產進行分類，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：

6.3.1 個人資料資產價值相同。

6.3.2 個人資料資產性質相同。

6.3.3 個人資料欄位要相同且資產數量較多。

6.4 評估項目

個人資料檔案風險評估下列幾個項目：

6.4.1 資產價值：個人資料檔案所含之個人資料範圍程度。

6.4.2 衝擊構面：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。

6.5 評估說明：

6.5.1 資產價值

個人資料檔案的資產價值，依據「國立宜蘭大學個人資料檔案清冊」（NIU-PIMS-D-007）的結果填入，每個檔案所含資產價值的等級分別給予低（1）、中（2）、高（3）與極高（4），四個等級評估。

資產價值	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（護照碼）及特種個人資料。
高（3）	1.含自然人之姓名及國民身分證統一編號（或護照碼），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（護照碼）及財務情況（如：薪資、局帳號），但不含特種個人資料。
中（2）	1.含自然人之姓名或國民身分證統一編號（護照碼），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。
低（1）	不含自然人之姓名及國民身分證統一編號（或護照碼）。

6.5.2 衝擊構面

為當個人資料檔案被竊取、竄改、毀損、滅失或洩漏等事故發生時，可能對各方面所產生的衝擊影響，依其可能的衝擊嚴重程度，給予低（1）、中（2）、高（3）、極高（4）等四個等級評估，取最高值。

項目／評估值	衝擊構面 1-衝擊影響	衝擊構面 2-可能性
1	個人資料檔案 500 筆以下，若發生損害賠償對學校財務影響範圍較小	已建立安全控管程序及相關文件，已落實。
2	個人資料檔案 500 筆 （含）以上 5000 筆以下，若發生損害賠償對學校財務影響範圍較小	未建立安全控管程序及相關文件，已實施安全控管。

3	個人資料檔案 5000 筆（含）以上 50000 筆以下，若發生損害賠償對學校財務影響範圍較大	已建立安全控管程序及相關文件，未實施安全控管。
4	所含個人資料檔案 50000 筆（含）以上，若發生損害賠償對學校財務影響範圍非常大	未建立安全控管程序及相關文件，亦無任何安全控管。

6.6 個人資料檔案風險評鑑

6.6.1 完成「國立宜蘭大學個人資料檔案清冊」（NIU-PIMS-D-007）資產價值評估後，接續對於所表列之清冊資產，進行風險評鑑作業。

6.6.2 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，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。

6.6.3 個人資料檔案風險值計算

(1) 依據依「國立宜蘭大學個人資料風險評鑑評估表」（NIU-PIMS-D-008）中資產價值、衝擊構面進行評估，以進行風險值計算。

(2) 風險值＝資產價值×（衝擊影響+可能性）

6.6.4 風險評鑑報告產出

個資保護執行小組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」，並建議可接受風險值，交由執行秘書決議。

6.7 個人資料檔案風險管理

6.7.1 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，需經執行秘書決議，並留存核決紀錄。

(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) 個人資料保護推動委員會（以下簡稱個保會）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。

6.7.2 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擬訂「國立宜蘭大學個人資料檔案風險處理計畫」(NIU-PIMS-D-009)，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應經由風險擁有者核准後執行，並由個資保護執行小組列入追蹤管理。

(3) 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「國立宜蘭大學個人資料檔案

風險處理計畫」(NIU-PIMS-D-009),並於預訂完成日期結束後,提報個保會審查。

(4) 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,提報個保會討論執行之成效與進度。

(5) 個資保護執行小組依據風險控管措施產出「適用性聲明書」。

6.7.3 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,須由個資保護執行小組(各單位個資保護聯絡窗口)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,並經由風險擁有者核准。

(2) 若處理後之風險值無法降至可接受風險值以下,應於個保會中提出討論,決定是否接受此風險或增加其他控制。

6.8 個人資料檔案風險管理評估審查

6.8.1 監控

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審。

6.8.2 持續改善

為維持本風險評鑑方法之有效性,個保會應:

(1) 每年檢討可接受風險值與「國立宜蘭大學個人資料風險評鑑評估

表」（NIU-PIMS-D-008）之衝擊構面與可能性構面項目。

(2) 將發生個資事故或遭遇個資訴訟判決相關資訊，納入「國立宜蘭大學個人資料風險評鑑評估表」（NIU-PIMS-D-008）衝擊構面與可能性構面，進行評估項目之檢討。

6.9 風險評鑑頻率

6.9.1 每年應至少執行 1 次風險評鑑。

6.9.2 當管理階層指示、作業環境、作業流程變更或系統重大異動後，應規劃排程執行風險評鑑。

7 相關表單

7.1 「國立宜蘭大學個人資料檔案清冊」（NIU-PIMS-D-007）。

7.2 「國立宜蘭大學個人資料風險評鑑評估表」（NIU-PIMS-D-008）。

7.3 「國立宜蘭大學個人資料檔案風險處理計畫」（NIU-PIMS-D-009）。

7.4 「適用性聲明書」（NIU-PIMS-D-027）。