致理科技大學

個人資料檔案風險評估與管理程序

機密等級：■一般 □敏感 □機密

編號：P-2-05

版本：2.0

發行日期：107 年 7 月 24 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
2.0	107.7.24	新增 BS 10012:2017 6.1.6 事前諮詢與授權條文、6.1.7 隱私權相關設計與預設條文相關內容，以及表單。	呂瑞茹	呂瑞茹

目錄

壹、目的：

為建立本校個人資料檔案之風險管理制度，提供共同遵行之風險評估標準，並規範高風險個人資料檔案之風險控制流程，特訂定本程序，以期有效降低個人資料檔案遭受損害之風險。

貳、範圍：

本校各項涉及個人資料之業務所產生的個人資料均適用之。

參、權責

會議/單位/人員	工作說明
個人資料保護推動委員會	1. 督導本校個人資料檔案風險評估與管理全般事宜
管理審查會議	1. 風險評估結果審查 2. 確認可接受風險程度 3. 風險處理計畫審查 4. 提供所需必要資源
個資保護聯絡窗口	1. 各單位校內風險管理與安全問題聯繫窗口 2. 協助單位擬定風險處理計畫 3. 個人資料檔案盤點 4. 個人資料檔案風險評估 5. 擬定並執行個人資料檔案風險處理計畫 6. 彙整並管制各單位個人資料檔案清冊

肆、定義：

一、 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。本校個人資料檔案依存在之形式區分為系統資料、電子資料及紙本資料三大類。

二、 系統資料：係指以應用系統存在之個人資料，並存放於伺服器資料庫中。

三、 電子資料：係指儲存於硬碟、磁帶、光碟、隨身裝置等儲存媒介以數位形態存在之電子檔案。

四、 紙本資料：係指以紙本形式存在之文書。

五、 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。

六、 威脅 (THREAT)：可能對個人資料資產或組織造成傷害之意外事件。

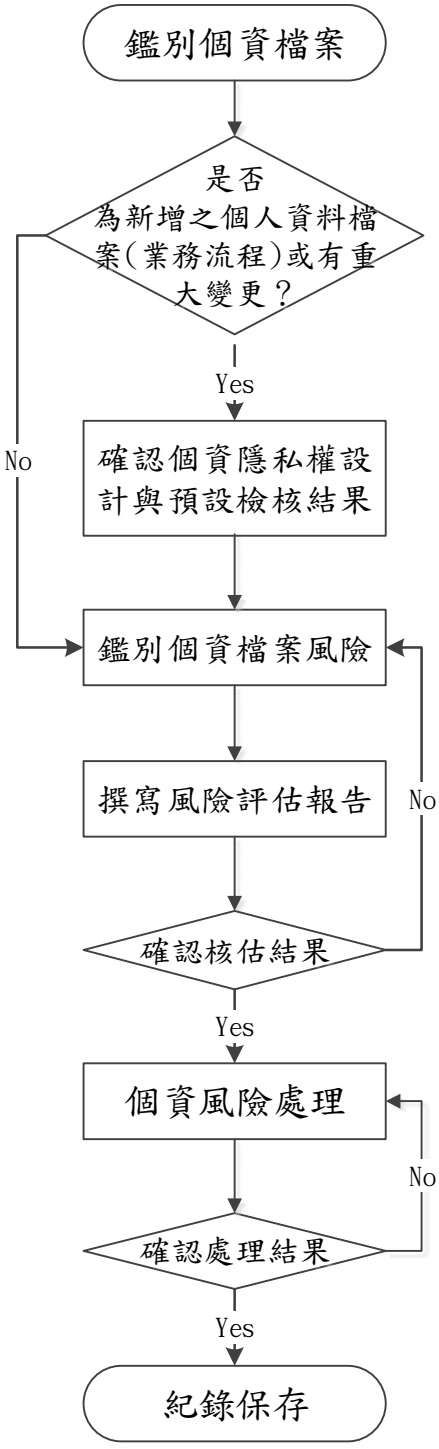
七、 弱點 (VULNERABILITY)：因個人資料資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。

八、 可接受風險：係指對於個人資料檔案發生損害，本校可容忍的最大程度。

九、 剩餘風險：係指個人資料檔案於施行相關控制措施後所剩餘的風險。

伍、作業內容：

一、 個人資料風險評鑑與處理管理流程

作業流程	權責單位	相關文件
	各單位個資保護窗口 各單位個資保護窗口 各單位個資保護窗口 各單位個資保護窗口 各單位個資保護窗口 單位主管 各單位個資保護窗口 單位主管 各單位個資保護窗口	個人資料盤點表 個人資料隱私權設計與預設檢核表 (107.7.24 新增) 個人資料檔案風險評估彙整表 個人資料檔案風險評估彙整表 個人資料風險評估報告 個人資料風險評估報告 個人資料風險處理計畫 個人資料風險處理計畫

二、 個人資料盤點及風險評估執行時機

（一） 本校每年定期至少執行一次個人資料盤點及風險評估作業。

（二） 於下列情形發生時，需對影響範圍內個人資料重新進行個人資料盤點及風險評估：

1. 學校組織、業務權責變更時。
2. 作業流程變更時。
3. 個人資料項目新增或異動時。
4. 發生重大資訊安全事件時。

三、 個人資料盤點

（一） 分析業務作業流程

個人資料盤點應由分析業務作業流程開始，由單位負責業務相關之程序與規範中（如：內部控制制度、標準作業程序、工作職掌、委外作業等），了解資訊的流向。

（二） 識別不同作業流程之個人資料項目

1. 從業務或服務作業的流程中，分析各服務內容之作業流程與應用系統清單，以找出含個人資料之業務或服務作業流程，並找出與業務相關各種存在型式之個人資料檔案。
2. 不同型式的資料，如書面紙本、電子檔案或備份資料等都應識別為不同的個人資料檔案。

（三） 識別個人資料檔案的相關屬性

識別出個人資料檔案的相關屬性，並填寫於個人資料盤點表中，相關屬性包含：

1. 個人資料項目基本資料：特定目的、個人資料類別、檔案型態、權責單位。
2. 個人資料項目生命週期活動：分析個人資料從蒐集、處理、利用、儲存、備份、傳輸、銷毀之活動及所需保存時間。
3. 個人資料項目相關人員：當事人、內部單位、委外單位、供應者。
4. 單位應彙整單位內個人資料盤點表，建立「個人資料盤點表」

四、 個人資料檔案風險評估

（一） 各單位應以「個人資料安全作業檢核表」確認單位對個人資料檔案保護是否落實。

（二） 依據「個人資料風險評估填寫說明」，對「個人資料盤點表」中所有個人資料檔案進行風險評估，並計算出每個個人資料檔案的風險值，並判斷風險處理之權責單位，彙整於「個人資料檔案風險評估彙整表」，經單位主管審核後，定期於管理審查會議中提報。

五、 決定可接受風險之風險值

（一） 於管理審查會議，各單位依前項之彙整表內容提出「個人資料檔案風險評估報告」，並依法令法規、客戶要求、合約、服務等級協議及營運需求等為基準，於管理審查會議中決定可接受風險程度之風險值。

（二） 各單位超過可接受風險程度之個人資料檔案，應於管理審查會議中提報風險處理計畫。

六、 個人資料檔案風險處理

（一） 各單位應就超過可接受風險程度之個人資料檔案提出「個人資料檔案風險處理計畫」，針對可能產生風險之威脅及脆弱點擬定安全控制措施，以期將風險降至可接受程度。

（二） 各單位將「個人資料檔案風險處理計畫」提報管理審查會議審查，於會議中同意處理計畫內容並提供所需資源後，依計畫執行改善。

（三） 管理審查會議應將「個人資料檔案風險處理計畫」列入追蹤管理，並定期確認其有效性。

（四） 若個人資料風險處理計畫無法將風險降低至可接受範圍內，應評估其它安控措施或有效性量測方式，以確保個人資料檔案可受到完善之保護。

七、 事前諮詢與授權

（一） 當各單位執行自然人的個人資訊之隱私權風險評估時，若個人資料檔案被鑑別為高風險時（參考本校 P-2-05-01 表單），且風險無法被減緩，應向主管機關事前諮詢與授權。

（二） 應依據主管機關事前諮詢與授權方式處理。

（三） 應保留事前諮詢、授權及處理之文件化資訊（如正式公文往返或 Email 聯繫紀錄等）。

八、 隱私權相關設計與預設

（一） 各單位新增與隱私權相關之業務流程或原有隱私權相關業務流程遇重大變更時，應先完成個人資料隱私權設計與預設檢核表（P-2-05-04），並保留該項業務檢核過程有關的文件化紀錄（如本校 P-2-05-04 表單及相關佐證資料）。

（二） 隱私權設計與預設應注意以下原則：

1. 預設最小化。
2. 盡可能使用去識別化資訊。
3. 功能與處置個人資訊的透明化考量。
4. 以組織化與技術行動實現：

（1）相稱於被識別化的風險。

（2）確保隱私權控制措施被適當實施為個人資訊保護。

（3）保留從設計著手保護隱私活動及結果的文件化紀錄。

九、 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	個人資料檔案風險評估彙整表	各單位	至少 3 年
2	個人資料風險評估報告	各單位	至少 3 年
3	個人資料風險處理計畫	各單位	至少 3 年

陸、 相關文件：

一、 個人資料風險評估填寫說明。(P-3-01)

柒、 使用表單：

一、 個人資料盤點表。(P-2-01-01)

二、 個人資料檔案風險評估彙整表。(P-2-05-01)

三、 個人資料風險評估報告。(P-2-05-02)

四、 個人資料風險處理計畫。(P-2-05-03)

五、 個人資料隱私權設計與預設檢核表。(P-2-05-04)