

亞東技術學院

個人資料風險評估與管理程序書

機密等級：一般

文件編號：PIMS-B-05

版 次：1.0

發行日期：2019/11/01

個人資料風險評估與管理程序書					
文件編號	PIMS-B-05	機密等級	一般	版次	1.0

目錄

1	目的	1
2	範圍	1
3	權責	1
4	名詞定義	2
5	作業內容	3
6	相關文件	7
7	使用表單	7

個人資料風險評估與管理程序書					
文件編號	PIMS-B-05	機密等級	一般	版次	1.0

1 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。

2 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。

3 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各項事宜
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

個人資料風險評估與管理程序書					
文件編號	PIMS-B-05	機密等級	一般	版次	1.0

	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風險處理計畫 6. 彙整並管制各單位個人資料檔案清冊
--	---

4 名詞定義

- 4.1 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。
- 4.2 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。
- 4.3 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。
- 4.4 紙本資料：係指以紙本形式存在之文書。
- 4.5 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。
- 4.6 威脅 (THREAT)：可能對個人資料資產或組織造成傷害之意外事件。
- 4.7 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。

個人資料風險評估與管理程序書					
文件編號	PIMS-B-05	機密等級	一般	版次	1.0

4.8 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。

4.9 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。

5 作業內容

5.1 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
 <pre> graph TD A([鑑別個資檔案]) --> B[鑑別個資檔案風險] B --> C[撰寫風險評估報告] C --> D{確認評估結果} D -- No --> B D -- Yes --> E[個資風險處理] E --> F{確認處理結果} F -- No --> E F -- Yes --> G([紀錄保存]) </pre>	<p>各單位個資保護聯絡 窗口</p> <p>各單位個資保護聯絡 窗口</p> <p>各單位個資保護聯絡 窗口</p> <p>單位主管</p> <p>各單位個資保護聯絡 窗口</p> <p>單位主管</p>	<p>個人資料盤點表</p> <p>個資檔案風險評估彙整表</p> <p>個資檔案風險評估彙整表</p> <p>個資檔案風險評估報告</p> <p>個資檔案風險評估報告</p> <p>個資檔案風險處理計畫</p> <p>個資檔案風險處理計畫</p>

個人資料風險評估與管理程序書					
文件編號	PIMS-B-05	機密等級	一般	版次	1.0
		各單位個資保護聯絡 窗口			

5.2 個人資料盤點及風險評估執行時機

5.2.1 本校每年至少執行一次個人資料盤點及風險評估作業。

5.2.2 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：

5.2.2.1 學校組織、業務權責變更時。

5.2.2.2 作業流程變更時。

5.2.2.3 個人資料項目新增或異動時。

5.2.2.4 發生重大個資安全事件時。

5.3 個人資料盤點

5.3.1 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。

5.3.2 識別不同作業流程之個人資料項目

5.3.2.1 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

個人資料風險評估與管理程序書					
文件編號	PIMS-B-05	機密等級	一般	版次	1.0

程，並找出與業務相關各種存在型式之個人資料檔案。

5.3.2.2 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。

5.3.3 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：

5.3.3.1 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。

5.3.3.2 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。

5.3.3.3 個人資料項目相關人員：當事人、內部單位、委外單位、供應者。

5.3.3.4 單位應彙整單位內個人資料盤點表，建立「個人資料盤點表」

5.4 個人資料檔案風險評估

5.4.1 各單位應確認個人資料檔案保護是否落實。

5.4.2 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

個人資料風險評估與管理程序書					
文件編號	PIMS-B-05	機密等級	一般	版次	1.0

風險值，並判斷風險處理之權責單位，彙整於「個人資料風險評估彙整表」，經單位主管審核後，定期於管理審查會議中提報。

5.5 決定可接受風險之風險值

5.5.1 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。

5.5.2 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。

5.6 個人資料檔案風險處理

5.6.1 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。

5.6.2 當個人資料檔案在風險評估中鑑別為高風險，且風險無法被減緩時，需向主管機關事前諮詢與獲得授權。

5.6.3 各單位將「個人資料風險處理計畫」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。

5.6.4 管理審查會議應將「個人資料風險處理計畫」列入追蹤管理，並定期確認其有效性。

個人資料風險評估與管理程序書					
文件編號	PIMS-B-05	機密等級	一般	版次	1.0

5.6.5 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度量測方式，以確保個人資料檔案可受到完善之保護。

5.7 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

6 相關文件

6.1 個人資料風險評估填寫說明。(PIMS-C-01)

7 使用表單

7.1 個人資料盤點表。(PIMS-B-03-D01)

7.2 個人資料風險評估彙整表。(PIMS-B-05-D-01)

7.3 個人資料風險處理計畫。(PIMS-B-05-D-02)

7.4 個人資料風險評估報告。(PIMS-B-05-D-03)