致理科技大學

個人資料事件管理程序

機密等級：■一般 □敏感 □機密

編號：P-2-06

版本：1.1

發行日期：106 年 6 月 15 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
1.1	106.6.15	當國內外其他組織發生 A 級重大個資外洩事件時之預防處理原則	林裕淇	呂瑞茹

目錄

壹、目的：

為建立快速、有效、有秩序的個人資料事件管理程序，以便降低或消除個人資料事故所可能帶來的傷害，強化個人資料事件處理能力，保護各項個人資料，並從中吸取經驗，以防範未來可能發生的個人資料事件。

貳、範圍：

本校各單位。

參、權責

單位/人員	工作說明
本校教職員工	1. 了解個人資料事件之通報程序 2. 對於已觀察到或懷疑可能發生的個人資料事件必須儘速通報個人資料保護聯絡窗口。
各單位個人資料保護聯絡窗口	1. 接收已觀察到或懷疑可能發生的個人資料事件回報 2. 判定個人資料事件種類、影響範圍、所需資源。 3. 判定個人資料事件是否需要通報，是否需要外力支援。 4. 評估個人資料事件處理所需時間，是否可能及時完成。 5. 個人資料事件協調、任務管制與進度追蹤。 6. 執行對上級通報作業，並於事件結束後回覆結案。 7. 協助個人資料事件應變與處理作業。 8. 由個人資料保護推動委員會副召集人擔任本校個人資料保護業務對外聯絡窗口，代表學校執行對外通報作業。

個人資料保護技術評估小組	1. 協助判定個人資料事件種類、影響範圍。 2. 單位內個人資料風險評估、損害預防及危機處理應變之通報。 3. 依授權執行損害減緩作業。 4. 執行個人資料事件應變與處理作業。 5. 對負責之業務範圍執行復原作業。 6. 國內外重大個資外事件之主被動蒐集、研析、建議或處理

肆、定義：

個人資料事故：

係指單一或一連串可能導致個人資料被竊取、洩漏、竄改或其它侵害之非預期個人資料事件，對本校已構成傷害，謂之個人資料事故。

伍、作業內容：

一、 為建立快速、有效、有秩序的個人資料事件管理程序，以便降低或消除個人資料事故所可能帶來的傷害，強化個人資料事件處理能力，並從中吸取經驗，據以防範未來可能發生的個人資料事件。

二、 個人資料事件類別

個人資料事件依發生原因分為 3 大類：

（一） 系統類

發生在網路環境、主機系統、個人電腦的事件，軟體、硬體與資訊紀錄相關者均屬之。例如系統故障、網路斷線、硬碟損毀、程式錯誤、機密檔案外洩等。

（二） 實體環境類

發生於實體環境內之事件，與實體文件及環境相關者均屬之。例如門禁故障、門窗未關、過載跳電、闖空門、重要紙本資料外流、火災等。

（三） 人員類

與人員相關之事件，例如人員作業疏失、意外事故、商業間諜混入偷竊

等。

三、 事件等級表事件等級

等級	影響程度	事件性質描述
D	小	當事人權利行使處理不當或對於本校個人資料管理所引起之抱怨或申訴
		個人資料外洩筆數在 200 筆以內
		外洩之個人資料僅含有一般性之識別資料
C	中	違反本校個人資料管理規範。當事人向高層主管提出抱怨或申訴
		一般個人資料外洩筆數在 201~10,000 筆之間 特種個人資料外洩筆數在 201~1,000 筆之間
		外洩之個人資料含有個人活動相關資料
B	大	上級單位、政府機構糾正、要求改善
		一般個人資料外洩筆數在 10,001~20,000 筆之間 特種個人資料外洩筆數在 1,001~5,000 筆之間
		外洩之個人資料含有金融財務相關資料
A	嚴重	違反法律要求、司法訴訟事件或公眾媒體報導影響本校聲譽。當事人向本校以外政府單位或相關機構檢舉或抱怨及申訴。
		一般個人資料外洩筆數在 20,001 筆以上 特種個人資料外洩筆數在 5,001 筆以上
		外洩之個人資料含有個資法第六條所定義之特種個人資料

四、 個人資料事件通報作業說明

（一） 由各個人資料權責單位聯絡協調窗口及個人資料保護推動委員會副召集人（擔任本校個人資料保護業務對外聯絡窗口），分別受理校內自行發現或校外單位告知本校之個人資料事件。

1. 各單位於發現個人資料事件時，應依據各種管道通知本校個人資料保護連

絡窗口，判斷是否發生個人資料事故。

2. 若並非個人資料相關狀況，應轉其它程序進行。

（二） 個人資料保護連絡窗口接獲個人資料事件通報後，須依所通報之內容進行瞭解，判斷是否為個人資料事故，將結果回覆個人資料事件通報單位，並填寫本校「個人資料事件處理單」。

1. 若確定為個人資料事故，須通報各個人資料權責單位承辦人，並於中央目的事業主管機關規定進行通報。

2. 若確定為個人資料事故，即通知相關個人資料權責單位進行處理，權責單位處理完成後，須將處理結果回覆本校個人資料保護業務對外聯絡窗口（主任秘書）。

3. 當發生個人資料事故，違反個人資料保護法，導致個人資料被竊取、洩漏、竄改或其它侵害者，應查明後以適當方式通知當事人並留下通報紀錄。此處之適當方式，依據個人資料保護法施行細則第二十二條，以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。

（三） 各個人資料權責單位應視事件種類及嚴重性，聯絡相關業務負責人及相關系統管理員，並視情況聯絡個人資料保護技術評估小組協助。

（四） 個人資料事件若涉及資訊安全問題，除依本程序進行外，另須依資訊安全事件管理程序書進行處理。

（五） 若為校外單位告知本校之事件或屬校外通報事件，應於事件處理完成後回報本校個人資料保護業務對外聯絡窗口（主任秘書）進行結案。

五、 個人資料事件損害減緩

（一） 為提高個人資料事故發生時之處理效率及應變能力，以釐清事故現況及影響範圍，防止損害擴大，應擬訂個人資料事故之「事故損害減緩計畫」，並於件等級達 B 級(含)以上時，考量啟動「事故損害減緩計畫」。

（二） 「事故損害減緩計畫」內容包含計畫之說明、系統架構、協力廠商清單、作業程序說明，以及含相關連絡資訊的「緊急連絡人員清單」。

（三） 各個人資料權責單位應擬定「事故損害減緩演練計畫」，並依計畫執行演練工作，以確保損害減緩計畫之正確性及有效性。

（四） 受個人資料事件影響之系統應依資訊安全事件管理程序書之指示進行應變處理，先停用或封鎖脆弱點之相關功能或元件，若屬無法停用之系統，應設置適當之監控機制。系統停用後須測試確認已恢復正常，並完成安全控制項目，確認脆弱點無法再被利用，系統才可上線運作，並視實際需求觀察系統運行一段時間，以確認系統持續正常運作。

六、 個人資料事件處理作業實施原則

（一） 若於非工作時間（例假日）發現個人資料事件，仍應依循程序通報處理。

（二） 識別事件所影響之資源與系統，供復原作業時參考。

（三） 處理作業時間應於指定時間完成，作業內容應記錄於「個人資料事件處理單」，並經由權責人員審視確認。

（四） 個人資料事件處理應確實做好證據保存工作。

（五） 應鑑別個人資料事件發生根本原因，以利事件處理作業。

（六） 若個人資料遭到人為竄改或失竊等涉及民、刑事案件時，應即時通知個人資料保護技術評估小組協助通報警政或檢調單位請求處理。

（七） 當個人資料事故為系統漏洞或脆弱點導致，應依資訊安全事件管理程序書處理，並透過網站資訊、技術支援單位(如廠商、技服中心等)查詢獲得解決方案，並執行修復動作。如暫時無解決方案，應先停用或封鎖脆弱點之相關功能或元件，避免脆弱點再度遭受利用。若屬無法停用之系統，應設置適當之監控機制。

（八） 若無法鑑別個人資料事故相關之系統的所有惡意行為(病毒感染、駭客入侵、木馬後門等)，無法確保完全清除並排除惡意程式或行為造成的影響，應嘗試重建一乾淨之系統，避免惡意程式持續影響系統運作。

（九） 為防止問題再度發生，個人資料事件須依「矯正預防管理程序」進行處理。

（十） 各個人資料權責單位應每月收集彙整個人資料事件，統計個人資料事件之數量、類別、影響範圍、發生部門/系統等，並分析其中的異常變化，以便掌握矯正及預防措施之有效性。

（十一） 當國內外其他組織發生 A 級重大個資外洩事件時，「個人資料保護技術評估小組」應主動協助本校業管單位進行預防處理，以有效防範類似事件在校內發生。

七、 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	個人資料事故損害減緩計畫	個人資料保護技術評估小組	至少 3 年
2	個人資料事故損害減緩演練計畫	技術評估小組	至少 3 年
3	個人資料緊急連絡人員清單	技術評估小組	至少 3 年
4	個人資料事件處理單	各單位	至少 3 年

陸、相關文件：

一、 國家資通安全通報應變作業綱要。

二、 資訊安全事件管理程序書。

三、 矯正預防管理程序。(P-2-09)

柒、使用表單：

一、 個人資料事故損害減緩計畫。(P-2-06-01)

二、 個人資料事故損害減緩演練計畫。(P-2-06-02)

三、 個人資料緊急連絡人員清單。(P-2-06-03)

四、 個人資料事件處理單。(P-2-06-04)