亞東學校財團法人亞東科技大學

個人資料事件管理程序書

機密等級：一般

文件編號：PIMS-B-07

版　　次：2.1

發行日期：2022/11/15

個人資料事件管理程序書					
文件編號	PIMS-B-07	機密等級	一般	版次	2.1

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	2019.11.01	ALL	個資保護執行小組	初版
1.1	2020.01.20	3,4	個資保護執行小組	修訂「事件等級表」的個資等級
2.0	2021.08.10	1	個資保護執行小組	因應學校改名進行改版
2.1	2022.11.15	5,9	個資保護執行小組	因應「私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法」修訂進行改版

目錄

個人資料事件管理程序書					
文件編號	PIMS-B-07	機密等級	一般	版次	2.1

1 目的

亞東學校財團法人亞東科技大學（以下簡稱本校）依據個人資料保護法要求，建立個人資料事件之預防、通報及應變等機制，促使個人資料事件能正確與即時的處理。

2 範圍

本校執行個人資料管理制度(PIMS)所發生個人資料事件之管理。

3 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。
主任秘書	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。
個資事件通報小組	1. 協助判定個人資料事件種類、影響範圍、所需資源。 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. 協助執行損害減緩作業。 4. 協助執行個人資料事件應變與處理作業。

	5. 建議個資失職人員適當之懲處。
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. 記錄個人資料事件，並於事件結束後回覆結案。 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. 協助個人資料事件應變與處理作業。 7. 有法律考量時，協助通報警政或檢調單位請求處理

4 名詞定義

4.1 個人資料事件與事故

係指單一或一連串違反個人資料保護法之規定，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。

5 作業內容

5.1 本程序包括評估、管理和記錄所涉及個人資料安全事件，並包括減緩任何安全事故所造成的損害的程序，以便降低或消除個人資料事故所可能帶來的傷害。

5.2 個人資料事件類別

個人資料事件依發生原因分為 3 大類：

5.2.1 系統類

發生在網路環境、主機系統、個人電腦的事件，軟體、硬體與資料紀錄相關者均屬之。例如駭客入侵、電腦病毒、機密檔案外洩等。

5.2.2 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。例如天災、火災、過載跳電、闖空門、重要紙本資料外流等。

5.2.3 人員類

與人員相關之事件，例如人員作業疏失、意外事故、個資偷竊等。

5.3 事件等級表

等級	影響程度	事件性質描述
非事故	無	經判定非個資事件或無影響
4	嚴重	上級單位、政府機構糾正、要求改善，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。
		一般個資外洩筆數在 20,001 以上 特種個資外洩筆數在 2,001 以上
3	大	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
		一般個資外洩筆數在 10,001~20,000 筆之間 特種個資外洩筆數在 1,001~2,000 筆之間
2	中	違反本校個人資料管理規範，程度較輕。
		一般個資外洩筆數在 1001~10,000 筆之間 特種個資外洩筆數在 101~1,000 筆之間
1	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
		一般個資外洩筆數在 1000 筆以內 特種個資外洩筆數在 100 筆以內

5.4 個人資料事件通報作業說明

5.4.1 由各單位個人資料保護聯絡窗口及執行秘書，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。

5.4.2 各單位於發現個人資料事件時，應通知本校個人資料保護聯絡窗口，判斷是否發生個人資料事故。

5.4.3 若並非個人資料相關狀況，應轉其它程序進行。

5.4.4 個人資料保護聯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。

5.4.5 若確定為個人資料事件，須填寫「個人資料事件處理單」，須通報各個人資料權責單位承辦人，另填寫「個人資料侵害事故通報與紀錄表」於 72 小時內回報主管教育機關，若未依時限內通報者，應附理由說明；並自處理結束之日起一個月內，將處理方式及結果，報主管教育機關備查。

5.4.6 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。

5.4.7 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。

5.4.8 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，並視情況聯絡個資事件通報小組協助。

5.4.9 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。

5.4.10 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（執行秘書）進行結案。

5.5 個人資料事件損害減緩及應變程序

組織遇有個人資料檔案發生遭人惡意破壞毀損、作業不慎、駭客攻擊或非法入侵等危害資訊安全之事故時，即應啟動應變作業處理程序，個資事故與應變處理程序如下：

5.5.1 準備階段

5.5.1.1 建立各項個資安全防護準備工作，如建立個資事件通報小組、個資防護設備部署作業、使用者個資安全認知訓練等。各項預防動作包括啟動必要之系統日誌，記錄個人資料存取時之活動，以期能監控並分析可疑事件。

5.5.1.2 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，應擬訂減緩個人資料事故之作業。

5.5.2 先期防護與分析階段

5.5.2.1 透過管理制度及資安設備的部署，並建立相對應的防護機制後，即開始進行偵測潛在性的資訊安全事件。

5.5.2.2 個資事故發生時，即按照組織之應變管理程序，由個資事件通報小組，判斷風險發生之來源及可能影響範圍，而必要證據之留存與保管，亦為現階段之重要關鍵點。

5.5.3 減緩個人資料事故之作業：

5.5.3.1 概估個資事故影響範圍、系統架構、協力廠商。

5.5.3.2 如屬非資訊面之個資外洩事故，應進行緊急因應措施，並迅速由個資事件通報小組進行通報。

5.5.3.3 如屬資訊面之個資外洩事故，應依組織之資訊安全業務持續計畫程序作業，迅速通報至資訊安全緊急應變小組。

5.5.3.4 在事件發生初期，投入適當的資源，以有效管理。

5.5.3.5 控制或減少風險，維護當事人權益。

5.5.3.6 適當的抱怨管理與授權的聯絡窗口說明。

5.5.4 事後處置階段

5.5.4.1 由個資事件通報小組偕同外部專家、委外廠商，進行辨識與分析事故發生來源與影響範圍，清查外洩資料影響範圍，進行鑑識分析以及必要證據留存。

5.5.4.2 有法律考量時，協助通報警政或檢調單位，以因應後續法律處理程序。

5.6 個人資料事件處理作業實施原則

5.6.1 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。

5.6.2 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。

5.6.3 個人資料事件處理應確實做好證據保存工作。

5.6.4 應鑑別個人資料事件發生根本原因，以利事件處理作業。

5.6.5 若個人資料遭到人為竄改或失竊等涉及民、刑事案件時，應即時通知個資事件通報小組協助通報警政或檢調單位請求處理。

5.6.6 若個資事件可能導致當事人權利和自由受到較高風險損害，應由授權之聯絡窗口通知當事人以下事項：

5.6.6.1 安全事件處理概況。

5.6.6.2 為減輕任何不利風險的行動的任何建議。

5.6.7 為防止問題再度發生，個人資料事件後續可依矯正預防作業進行處理。

5.6.8 個人資料之事件懲處管理

「個資事件通報小組」查明相關人員疏失之責任歸屬後，視情節

之輕重建議適當之懲處。

5.6.9 媒體處理原則

本校所發生之個人資料事件若已經由媒體報導曝光後，應由本校授權之對外聯絡窗口統一對外發言及公布相關訊息，其他單位及同仁嚴禁以任何形式對外提供及發表任何訊息或意見。

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	個人資料事件處理單	文管中心	至少 5 年
2	個人資料侵害事故通報與紀錄表	文管中心	至少 5 年

6 相關文件

6.1 個人資料安全管理程序書。(PIMS-B-08)

7 使用表單

7.1 個人資料事件處理單。(PIMS-B-07-D-01)

7.2 個人資料侵害事故通報與紀錄表。(PIMS-B-07-D-02)