大華科技大學

個人資料事件管理程序

機密等級：限閱

文件編號：B-006

版　　次：1.1

發行日期：104.05.19

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	103.05.27		蕭崇惠	初版
1.1	104.05.19		個人資料保護推動小組	修訂者修改為個人資料保護推動小組

個人資料事件管理程序					
文件編號	B-006	機密等級	限閱	版次	1.1

目　　錄

個人資料事件管理程序					
文件編號	B-006	機密等級	限閱	版次	1.1

一、目的：

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

二、範圍：

本校各單位。

三、權責：

單位/人員	工作說明
單位同仁	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資保護連絡窗口。
個資保護連絡窗口	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.判定個資事件是否需要通報，是否需要外力支援。 4.評估個資事件處理所需時間，是否可能及時完成。 5.個資事件協調、任務管制與進度追蹤。 6.執行對上級及對外通報作業，並於事件結束後回覆結案。 7.協助個資事件應變與處理作業。
單位資料保護代表 業務負責人	1.協助判定個人資料事件種類、影響範圍。 2.單位內個資風險評估、損害預防及危機處理應變之通報。

四、名詞定義：

個資事故：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資事件，對本校已構成傷害，謂之個資事故。

五、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，以降低或消除個人資料事故所可能帶來的傷害，強化個資事件處理能力，並從中吸取經驗，以防範未來可能發生的個人資料事件。

(二).個資事件類別

個資事件依發生原因分為 3 大類：

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。

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。

3.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).個資事件通報作業說明

1.由個資保護連絡窗口,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).各單位於發現個資事件時,應依據各種管道通知本校個資保護連絡窗口，判斷是否發生個資事故。

(2).若並非個資相關狀況，應轉其它程序進行，例如「內控程序_資安事件管理」

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

(1). 若確定為個資事故,須通報個人資料保護推動小組負責人及校安中心，並於教育機構資安通報平台進行通報。

(2). 若確定為個資事故，即通知相關權責單位進行處理，權責單位處理完成後，須將處理結果回覆個資保護連絡窗口。

(3). 當發生個資事故,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下通報紀錄。此處之適當方式，依據個資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。

3. 權責單位視事件種類及嚴重性,須聯絡相關業務負責人及相關系統管理員，並視情況聯絡技術專家協助。

4. 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「內控程序_資安事件管理」進行處理。

5. 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進行結案。

(四). 個資事件損害減緩

1. 為提高個資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，應擬訂個資事故之「損害減緩計畫」

2.「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」

3. 個人資料保護推動小組應擬定「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。

4. 受個資事件影響之系統應依「內控程序_資安事件管理」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。

(五).個資事件處理作業實施原則

1.若於非工作時間（例假日）發現個資事件，仍應依循程序通報處理。

2.識別事件所影響之資源與系統，供復原作業時參考。

3.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。

4.個資事件處理應確實做好證據保存工作。

5.應鑑別個資事件發生根本原因，以利事件處理作業。

6.若個資遭到人為竄改或失竊等涉及民、刑事案件時，應即時通知校安中心協助通報警政或檢調單位請求處理。

7.當個資事故為系統漏洞或脆弱點導致,應依「內控程序_資安事件管理」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，應先停用或封鎖弱點之相關功能或元件,避免弱點再度遭受利用。若屬無法停用之系統, 應設置適當之監控機制。

8.若無法鑑別個資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。

9. 為防止問題再度發生，個資事件須依「矯正預防管理程序」進行理。

10. 個人資料保護推動小組每月收集彙整個人資料事件,統計個資事件之數量、類別、影響範圍、發生部門及系統等，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。

六、相關文件：

(一). 國家資通安全通報應變作業綱要。

(二). 內控程序_資安事件管理。

(三). 矯正預防管理程序。

七、使用表單：

(一). 個人資料事故損害減緩計畫。

(二). 個人資料事故損害減緩演練計畫。

(三). 緊急連絡人員清單。

(四). 個人資料事件處理單。