國立臺南藝術大學

個人資料保護緊急應變處理作業說明書

機密等級：一般

文件編號：PIMS-C-002

版　　次：2.4

發行日期：115.08.13

個人資料保護緊急應變處理作業說明書					
文件編號	PIMS-C-002	機密等級	一般	版次	2.4

修訂紀錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
2.0	106 年 9 月 26 日	新增	個資管理委員會行政小組	依「教育體系資通安全暨個人資料管理規範」、ISO 27001：2013 版制定
2.1	106 年 11 月 9 日	p5.p7	行政小組	修訂個人資料事故應變演練計畫及報告名稱
2.2	112 年 8 月 2 日	P2~p7	行政小組	個人資料窗口更名為個人資料保護專責人員
2.3	113 年 07 月 17 日	P1~P7	個資管理委員會行政小組	修正部分文字，並將「個資」文字統一修正為「個人資料」
2.4	115 年 08 月 13	P2、P4	個資管理委員會執行小組	1.調整行政小組為執行小組並調整流程圖 2.調整部分文字排版

目錄

個人資料保護緊急應變處理作業說明書					
文件編號	PIMS-C-002	機密等級	一般	版次	2.4

壹、目的

國立臺南藝術大學(以下簡稱本校)為建立個人資料事故管理作業準則，並規範事故處理之作業事項，針對個人資料侵害之情形，決定其影響範圍及緊急程度，並能快速解決問題，確保事故能有效處理，特訂定「個人資料保護緊急應變處理作業說明書」，以茲遵循。

貳、參考依據

一、教育體系資通安全暨個人資料管理規範

二、PIMS-B-007 個人資料矯正預防管理程序書。

三、PIMS-B-002 個人資料文件管理程序書。

參、適用範圍

無論來自於人為故意或不經意的，或不可抗力的因素，任何導致本校個人資料管理異常狀況均適用之。

肆、權責

一、個人資料保護管理委員會（以下簡稱個資管理委員會）

(一)負責個人資料事故處理與預防。

(二)負責個人資料保護資源協調與流程改善。

(三)負責監督重大／緊急事故及稽核缺失的矯正措施之實施，並確認預防措施之有效性。

二、個資管理委員會執行秘書

(一)個人資料保護業務之協調聯繫及緊急應變通報。

(二)督導個人資料事故通報應變作業執行狀況。

三、個資管理委員會執行小組

(一)「個人資料保護法」(以下簡稱個資法）第十條及第十一條第一項至第四項所定依法或依當事人請求事項之考核。

(二)個資法第十一條第五項及第十二條所定通知事項之考核。

(三)本校個人資料保護方針及政策之執行、單位內個人資料保護之自行查核。

(四)辦理事件辨識、抑制、排除及回復作業。

(五)辦理本校各單位之個人資料損害預防及危機處理應變之通報。

(六)協助辦理本校各單位之個人資料保留與處置。

(七)建立並統籌個人資料事故聯繫窗口。

(八)由個資管理委員會指派執行小組擔任本校個人資料保護專責人員。

四、本校所有同仁

(一)協助配合各類個人資料事故之報告與處理。

(二)應瞭解個人資料事故應變通報流程，並協助通報相關權責單位。

五、委外廠商與人員

遵守法規及本校相關個人資料保護管理制度規範。

伍、定義

個人資料事故，係指單一或一連串機率可能危害與威脅個人資料安全之非蓄意或非預期的個人資料事故；簡而言之，泛指對本校已構成傷害之事故。例如：

一、個人資料檔案遭遇竊取、竄改、毀損、滅失或洩漏等相關事故。

二、洩漏個人資料或違反個人資料政策之故意行為或重大人為疏失。

三、販賣個人資料圖利。

四、個人資料檔案遭受誤用。

五、超過蒐集之特定目的處理或利用。

六、未經同意蒐集個人資料。

七、個人資料未應當事人請求修改、刪除、停止使用、製給複製本及閱覽權利。

陸、作業說明

一、建立個人資料事故通報及受理程序

(一)本校應建立完整之內部個人資料事故通報流程，當發生個人資料外洩時必須告知當事人並留下通報紀錄，若有通報而無相關通報記錄，事後將究責。

(二)個人資料事故其通報方式依據本作業說明書「個人資料事故通報及受理流程」辦理。

(三)接獲個人資料事故通報後，需依所通報之內容進行處理，並填寫本校「PIMS-D-025-個人資料侵害事故通報與紀錄表」。

(四)當違反個資法規定，導致個人資料被竊取、洩漏、竄改或其他侵害者，

應於查明後以適當方式通知當事人。

(五)應建立通報機制，確保所使用的方式（例如電話、簡訊、郵寄、E-mail等）可以通知到當事人，並留下紀錄。

(六)個人資料事故通報單位依據各種管道向本校個人資料保護專責人員進行通知，由個人資料保護專責人員判斷是否為個人資料事件，若確定為個人資料事件後，將問題轉予權責單位進行處理，待權責單位處理完成後，將處理結果回覆個人資料保護專責人員 ，由個人資料保護專責人員判斷事件是否違反個人資料保護法，並回覆個人資料事故通報單位，且保留相關紀錄。

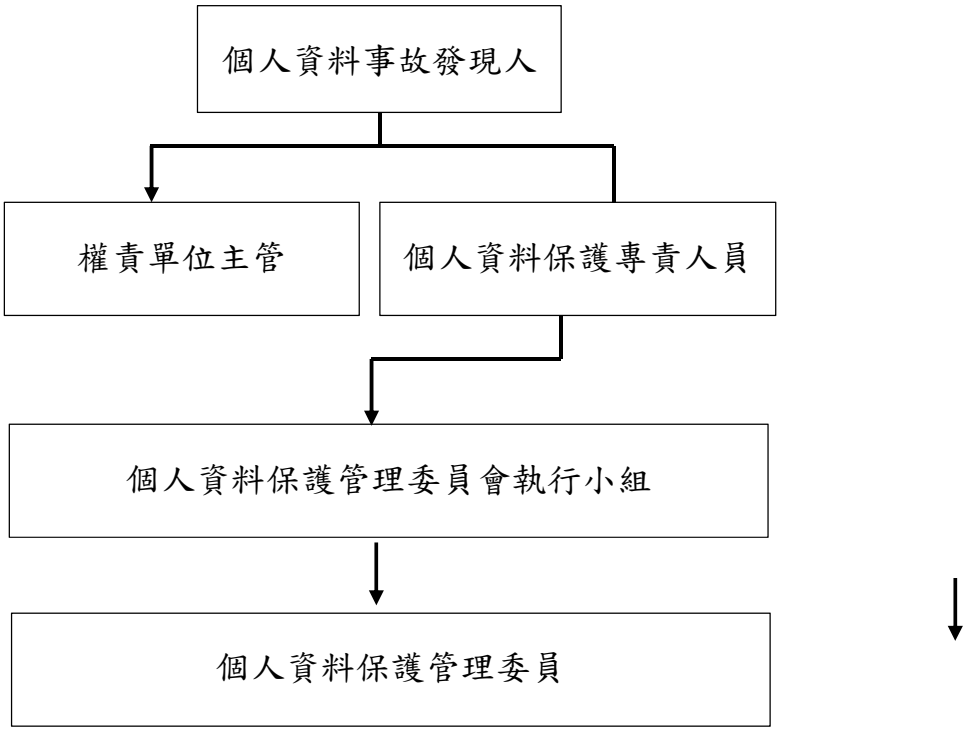
(七)個人資料事故之當事人通報及受理程序詳本校「PIMS-D-024-個資事故通報及受理流程」。

(八)若確實是由內部處理不當導致當事人個人資料洩漏、損失及毀損等情形，將依個資法第二十八條進行損害賠償。

二、個資事故通報

(一)各單位於發現個人資料遭侵害時，應通知個人資料保護專責人員 ，由個人資料保護專責人員與個資管理委員會執行小組判斷是否發生個人資料事故。

(二)事故發生時，應依下列流程進行通報，以便即時處理與解決。



三、通報原則

(一)個人資料事故發生時，應依通報順序逐級陳報。

(二)當上述任何一層級人員無法依層級順序被通報時，負責通報人員應往上一層級逕行陳報，以確保通報程序之即時性。

四、判斷個人資料事故

(一)個人資料保護專責人員接獲相關個人資料案件通知時，應立即協同相關人員蒐集相關跡證，初步判斷是否發生個人資料事故及其影響程度與範圍。

(二)若經判斷為個人資料事故，事故處理之業管單位應立即依據「個人資料事故通報及受理流程」，啟動個人資料應變措施相關處理作業。

(三)個人資料保護專責人員應將相關異常通知、事故判斷及處理情形等相關資訊，確實記錄於「PIMS-D-025-個人資料侵害事故通報與紀錄表」，並陳報權責單位主管審核。

五、記錄個人資料事故，啟動應變措施

個人資料應變措施應符合限制、處理、復原等三階段的事故處理原則，

說明如下：

(一)針對可即時解決之個人資料事件，業務權責單位陳報主管審核後， 並通報個人資料保護專責人員。

(二)若個人資料遭到人為竄改或失竊等涉及民、刑事案件時，應即時通報警政或檢調單位請求處理。

(三)事故處理作業所留存之相關紀錄應至少保留 1 年備查或依據本校【PIMS-B-002-個人資料文件管理程序書】規定控管。

(四)為提高個人資料侵害發生時之處理效率及應變能力，應擬定個資事故演練計畫，並定期實施演練作業及計畫內容維護，遇事故發生時能有因應之對策且不慌亂。

1. 個人資料侵害事故之演練測試

（1）「個資管理委員會」每年至少執行一次緊急應變演練，以確保計畫之正確性及有效性。

（2）訂定演練模式及週期

（3）演練單位個人資料侵害事故之演練測試，應依個人資料作業流程業務重要性，擬定個人資料作業流程演練時程表執行演練，以確保有效性並訂定「個人資料事故應變演練計畫」。個人資料侵害事故之緊急計畫之演練可擇以下一種或數種測試模式：

A. 書面模擬演練（Desktop Exercise）（無法進行實況演練者）。

B. 資料回復演練（Data Recovery）。

C. 情境模擬演練（Scenario Simulation）。

D. 實況演練（Simulation)。

E. 預警／無預警演練。

2. 演練計畫宜包含以下項目：

（1）演練目的與範圍。

（2）演練情境說明。

（3）演練時程規畫。

（4）演練順序及步驟。

（5）演練所需資源清單。

（6）參與單位及負責人員清單。

（7）協力廠商聯絡清單。

（8）模擬通報機制。

3. 演練計畫之執行於演練過程，應留存紀錄。

4. 演練報告

（1）演練結束後，演練單位應就演練過程，加以記錄並檢討演練過程中發生之問題及改善事項等，彙整於「個人資料事故應變演練報告」陳單位主管核定後留存備查，以便後續追蹤。

（2）演練單位應於「個資管理委員會」報告演練測試之執行情形。

(五)若因個資事故連帶影響其他系統或資訊基礎建設運作時，應依據本校「PIMS-B-007-個人資料矯正預防管理程序書」填寫「PIMS-D-020-個人資料管理制度矯正預防處理單」進行後續處理。

六、確認狀況排除

(一)個人資料事故處理人員於處理完成後，應確認應變措施之有效性， 並回報個人資料保護專責人員及業務權責單位主管，視情況調整應變措施。

(二)個人資料事故發生之業務權責單位主管於初步認定事故排除後，仍應嚴密監控相關資訊，並進行必要之安全清查，防止潛伏之可疑行為再發生。

(三)個人資料事故確認排除後，業務權責單位應再回報個人資料保護專責人員後續處理情形，且由其通知本校受事故影響之相關單位或回報上級單位。

(四)個人資料保護專責人員應留存紀錄，並決定是否通報主管機關或要求業務權責單位通知當事人。

(五)業務權責單位應儘速將損失彙整後通知個人資料保護專責人員，由個人資料保護專責人員提供予個資管理委員會，負責協助本校召集人對外說明情況與處置方式。

七、檢討及改善

(一)個人資料事故確認處理完成後，事故發生單位應檢討現行安全控制措施之完整性，並適當修訂相關作業管理規範或建置控制措施，且於必要時召開檢討會議。

(二)事故發生單位應於事故處理完畢後，進行相關矯正預防措施， 避免同類型之個人資料事故重複發生。

(三)各單位權責主管應監督個人資料事故之後續處理及安全控制之有效性。

(四)個人資料事故之發生單位應為個人資料稽核作業之重點，並列入追蹤管理。

(五)由個人資料保護專責人員彙整「PIMS-D-025-個人資料侵害事故通報與紀錄表」，並在無牽涉個人隱私與本校業務機密之情況，將事件發生原因、過程、處理方式、注意事項及改善建議等內容，以網站或電子郵件等方式提供予本校員工，以做為內部個人資料保護安全宣導及事故預防之參考。

柒、相關表單

一、PIMS-D-024 個資事故通報及受理流程。

二、PIMS-D-025 個人資料侵害事故通報與紀錄表。

三、PIMS-D-027 個人資料事故應變演練計畫。

四、PIMS-D-028 個人資料事故應變演練報告。