國立臺北科技大學
National Taipei University of Technology

個人資料保護應變處理作業辦法

文件編號：PIMS-C-002

機密等級：限閱

版次：1.0

發行日期：104.05.06

本文件修訂權為個人資料保護管理委員會

本文件歷次變更紀錄：

版次	修訂日期	修訂頁次	修訂內容摘要
1.0			第一版

目錄

1 目的

依據「個人資料保護法」(以下簡稱個資法)、「個人資料保護法施行細則」、個人資料管理制度（PIMS）BS 10012：2009 標準及國立臺北科技大學（以下簡稱本校）「個人資料保護管理政策」等相關規定，制訂本校個人資料發生洩漏、損失及毀損等狀況時之通報與應變處理等控管方式。

2 適用範圍

本校所有書面或電子之個人資料均適用之。

3 權責

3.1 個人資料保護管理委員會

3.1.1 負責個資事故異常處理與預防。

3.1.2 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。

3.2 個資保護小組

3.2.1 依個資法第 10 條及第 11 條第 1 項至第 4 項所定依法或依當事人請求事項之落實與考核。

3.2.2 依個資法第 11 條第 5 項及第 12 條所定通知事項之落實與考核。

3.2.3 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。

3.2.4 單位內個人資料損害預防及危機處理應變之通報。

3.2.5 個資事故處理聯繫窗口。

3.3 執行秘書

3.3.1 協調個資保護小組執行個資保護及緊急事故處理等相關作業。

3.4 個資保護小組組長

3.4.1 個人資料保護業務之協調聯繫及緊急應變通報。

3.4.2　重大個人資料外洩事件之客戶聯繫單一窗口。

3.5　全體員工

3.5.1　各類個人資料保護事故之報告與處理。

3.5.2　事故發生時，迅速通報個資事故權責單位。

3.5.3　協助異常事故之配合處理。

3.6　委外廠商與人員

遵守相關個人資料管理制度規範。

4　名詞定義

4.1　個資事故

單一或一連串可能危害與威脅個資安全之非蓄意或非預期的個資事故；簡而言之，泛指對組織已構成傷害之事故。

4.1.1　個人資料檔案遭遇竊取、竄改、毀損、滅失或洩漏等相關事故。

4.1.2　洩漏個人資料或違反個資政策的故意行為或重大人為疏失。

4.1.3　販賣個人資料意圖營利。

4.1.4　個人資料檔案遭受誤用。

4.1.5　未符合個資法的特定目的外之處理或利用。

4.1.6　依個資法應經當事人書面同意卻未經同意蒐集個人資料。

4.1.7　個人資料未給予當事人請求修改、刪除、停止使用、製給複製本及閱覽權利。

5　作業內容

5.1　建立個資事故通報及受理程序。

5.1.1　本校應建立完整之內部個人資料事故通報流程，當發生個資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，事後將對相關人員究責。

5.1.2　個資事故其通報方式依據 5.3.2 辦理。

5.1.3　個資事故通報後，需依所通報之內容進行處理，達個資事故認定原則之事故處理情形，由電話受理人員或由 e-mail 受理之個資保護小組成員寫本校「個人資料事故通報單」辦理。

5.1.4　違反「個人資料保護法」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。

5.1.5　應建立通報機制，確保通知的適當方式（例如電話、簡訊、郵寄、email 等）可通知到當事人，並留下紀錄。

5.1.6　個資事故之當事人通報及受理程序詳本校「個人資料事故通報及受理流程」。

5.2　建立個資事故分析及處理程序

5.2.1　當事人對其個人資料的查詢請求，於提出個資查詢需求時，應填寫「資訊服務申請表」經個人資料保護管理委員會核准後，以回應當事人對其個人資料的查詢請求。

5.2.2　個資保護小組成員應於查詢後以適當方式提供當事人並留下紀錄。

5.2.3　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「個人資料矯正預防程序書」填寫「矯正預防處理單」進行後續處理。

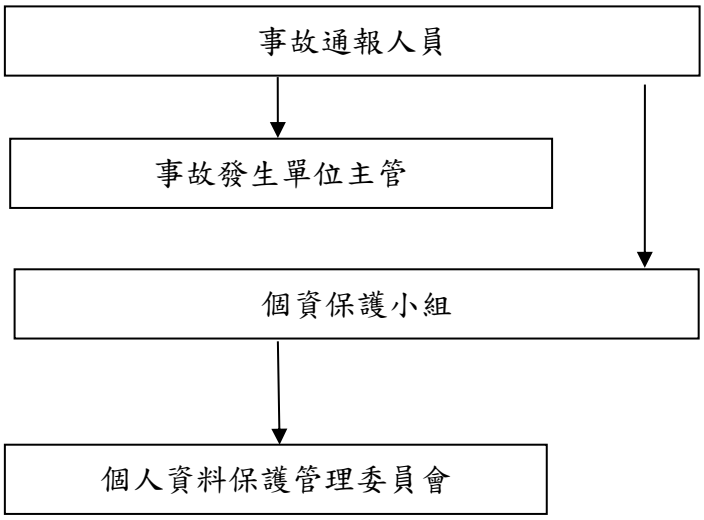
5.2.4　若確實是由內部處理不當導致當事人個人資料洩漏、損失及毀損等情形，將依個資法第 4 章第 29 條進行損害賠償。

5.3　個資事故通報

5.3.1　人員於發現相關異常時，應立即通報事故發生單位的人員及主管，並由該單位人員通知個資保護小組，並協助判斷是否發生個資事故。

5.3.2　事故發生時，應依下列流程進行通報，以便即時處理與解決。必要時應依相關法規通知主管機關。並依個資法第 12 條規定於違反個資法規定致個人資料被竊取、洩露、竄改或其他侵害者，查明後以適當方式通知當事人，通知內容應包括個人資料被侵害之事實及已採取之因應措施。

個資事故內部通報流程



5.3.3　通報原則：

5.3.3.1 個資事故發生時，應依通報順序逐級陳報。

5.3.3.2　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。

5.3.3.3 個資保護小組應維護各相關人員最新之緊急聯絡電話。

5.3.3.4　必要時應依相關法規通知主管機關。並依個資法第 12 條規定於違反個資法規定致個人資料被竊取、洩露、竄改或其他侵害者，查明後以適當方式通知當事人，通知內容應包括個人資料被侵害之事實及已採取之因應措施。

5.4　判斷個資事故

5.4.1　權責人員接獲相關異常通知時，應立即協同個人資料保護管理委員會蒐集相關跡證，初步判斷是否發生個資事故及其影響程度與範圍。

5.4.2　若經判斷為個資事故，事故處理之權責單位應進行相關處理作業，並將處理情形記錄於「個人資料事故通報單」。

5.5 記錄個資事故，啟動個資應變措施

應變措施應符合限制（避免範圍擴大）、處理、復原等三階段的事故處理原則。

5.5.1 針對可即時解決之個資事件，權責單位負責人應於事故處理完畢後，陳報權責單位主管審核。

5.5.2 若個資遭到人為竄改或失竊等涉及民、刑事案件時，應即時通報警政或檢調單位請求處理。並應依相關法規通知主管機關。且依個資法第 12 條規定於違反個資法規定致個人資料被竊取、洩露、竄改或其他侵害者，查明後以適當方式通知當事人，通知內容應包括個人資料被侵害之事實及已採取之因應措施。

5.5.3 事故處理作業所留存之相關紀錄應依據本校「文件管理程序書」規定控管。

5.6 確認狀況排除

5.6.1 個資事故負責人員於處理完成時，應確認應變措施之有效性，隨時回報個資保護小組及事故發生單位權責主管，並視情況調整應變措施。

5.6.2 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，防止潛伏之可疑程式、行為發生或散播。

5.6.3 個資事故確認排除後，事故主管人員應通知受事故影響之相關單位或人員；個資保護小組應回報上級單位。

5.7 檢討及改善

5.7.1 個資事故確認處理完成後，事故發生單位應檢討現行管理措施之完整性，並適當修訂相關作業管理規範或建置控制措施，且於必要時應召開檢討會議。

5.7.2 事故發生單位應於事故處理完畢後，應進行相關矯正預防措施，以避免同類型之異常事故重複發生。

5.7.3 個人資料保護管理委員會應監督重大/緊急事故之矯正措施之實施，並確認預防措施之有效性。

5.7.4 個人資料保護管理委員會應監督一般個資事故之後續處理及其有效性。

5.7.5 重大/緊急個資事故之矯正預防措施及事故發生單位應為個人資料內部稽核

作業之重點，並列入追蹤管理。

6 參考文件

6.1 個人資料保護法。

6.2 個人資料保護法施行細則。

6.3 BS 10012:2009 標準。

6.4 個人資料保護管理政策。

6.5 個人資料保護組織程序書。

6.6 個人資料矯正預防程序書。

6.7 個人資料文件管理程序書。

7 相關表單

7.1 個人資料事故通報單。

7.2 個人資料事故通報及受理流程。

7.3 資訊服務申請表。

7.4 矯正預防處理單。