國家科學及技術委員會新竹科學園區管理局個資事故通報處理及應變程序

中華民國107年10月9日科技部新竹科學工業園區管理局竹秘字第1070029987號函訂定
中華民國108年12月18日科技部新竹科學園區管理局竹秘字第1080037320B 號函修正，並修正名稱為「科技部新竹科學園區管理局個資事故通報處理及應變程序」
中華民國111年7月29日國家科學及技術委員會新竹科學園區管理局竹秘字第1110024890號函修正
中華民國112年9月11日國家科學及技術委員會新竹科學園區管理局竹秘字第1120030940號函修正

一、適用範圍

適用於所有與本局營運相關之個資事件及行為。本局人員及與本局成立契約關係或類似契約關係之第三人,包括但不限於供應商、承包商、約聘人員及顧問，如於執行本局相關業務時發生個資安全事故，皆應適用本程序。

二、定義

本程序所稱個資安全事故，係指：

(一)個資發生被竊取、竄改、毀損、滅失、洩漏或其他侵害等事故。

(二)發生違反個資相關法令或本局個資保護相關規定之情形。

(三)其他涉及個資安全之事故。

三、通報及應變程序(附圖一)

(一)個資安全事故之通報程序

1. 於獲悉個資當事人抱怨、間接獲知個資因竊取、竄改、毀損、滅失、洩漏或其他侵害等，或發現個資安全事故已發生或可能發生，應立即檢視事件重大性並於知悉或發現之時起二十四小時內通報個人資料保護管理執行小組（以下簡稱「個資執行小組」)。

2. 事件具有緊急重大性，且涉及資訊設備之緊急修復時，同仁應於通報個資執行小組後，迅速協助知會相關處理單位（例如：國家科學及技術委員會資訊處竹科辦公室）進行處理。

3. 同仁於通報後,應即將通報內容及初步處理狀況記錄於「個資安全事故紀錄單」(附表一)中，並送單位主管簽核後，

由個資執行小組保存。

(二)個資安全事故之緊急處理程序(附圖二)

1. 個資執行小組收到通報後，若認該事件將使個資可能在短時間內遭到毀損、滅失、洩漏或其他侵害時，或如不進行緊急處理可能使得損害快速擴大時，應即通知相關人員或協力廠商進行緊急處理。

2. 緊急處理措施

(1) 應以業管單位為原則，惟個資執行小組視情況需要，得進行必要之指揮監督。

(2) 緊急處理時，應採取免於個資繼續受到毀損、滅失、洩漏之保護措施，例如於災難現場快速打包個資，並進行清點。

3. 緊急處理後，個資執行小組應根據事故狀況進行調查、通報個資當事人、維護個資正確性、更正錯誤、改善整體環境或通報主管機關等作業。

4. 緊急處理後，個資執行小組應將處理情形填載於「個資安全事故紀錄單」。

5. 關於事件發生後之個資正確性維護、錯誤之更正或整體環境之改善，由個資執行小組責成相關單位進行後續處理。相關單位於後續處理完成後,應於「個資安全事故紀錄單」填載改善措施及從事故中學習到的經驗或課題。

6. 如因事故排除而有重新蒐集、處理及利用個資之必要，亦應重新告知個資當事人及取得其書面同意。

(三)個資安全事故處理程序

1. 於事故初步處理完畢後，個資執行小組應依下列方式，查明事故發生之原因：

(1) 內部調查

A. 資訊單位：清查可能導致事故發生或資料外洩之缺口，透過檢視相關 Log 紀錄，如電子郵件傳送紀錄、資料下載紀錄等，分析可能導致事故之人

員、時間及方式。

B. 稽核單位：清查事故發生相關之作業程序，透過作業流程檢視、文件檢視、單位主管覆核紀錄等，以指出可能之問題所在。

C. 各單位主管：檢視其單位之相關書面文件是否遭竊、非授權複製、拷貝等情況。

(2) 外部調查

A. 得委託外部顧問對本局進行鑑識稽核作業，透過特定檢視程序，對引起事故發生之可能處進行流程查訪，以確認問題之所在。

B. 得委託徵信單位，對於本局內部可能導致事故之特定人員或外部有心人士進行可能犯罪行為進行蒐集、監視，並提供本局蒐集、分析之結果。

C. 詢問個資當事人得知受害之相關情形和管道，並據以了解事件發生原因。

D. 詢問導致事故發生之本局內、外部人員及其曾接觸之人員。

2. 查明事故發生原因後，個資執行小組應填寫「個資安全事故通知當事人紀錄單」(附表二)，並依照個人資料保護法第十二條所要求，透過適當方式通知個資當事人，通知的內容應包括個資當事人個資被侵害之事實及本局已採取之因應措施，以及後續提供查詢及協助之方式。

3. 如符合相關法令須申報之規範，個資執行小組另應依法向主管機關提出申報。

4. 事故發生後之個資正確性維護、錯誤之更正或整體環境之改善,由個資執行小組責成相關單位進行討論及後續處理。相關單位於後續處理完成後，於「個資安全事故紀錄單」填載改善措施及從事故中學習到的經驗或課題。

5. 如因事故排除而有重新蒐集、處理及利用個資之必要，亦應重新告知當事人及取得其書面同意。

四、獎懲原則

(一)員工如遵守本程序並通報個資安全事故，倘經個資執行小組判斷該通報行為有效防止個資安全事故之發生或有效降低損害者，應給予適當之獎勵。

(二)員工如有隱瞞個資安全事故之行為，而致本局或負責人受有損害或有損害之虞，應給予警告或懲處。

五、通報(知)注意事項

(一)機關內進行各層級之通報,視法律規定通報各事業主管機關、當地縣市政府，最重要是通知個資當事人。

(二)若個資事件影響範圍不大，機關可在初步擬定說明函以及道歉函後，各別通知當事人。通知內容務必讓當事人了解機關有誠意解決問題，並負起一切賠償責任，儘量避免個人訴訟或團體訴訟成案，影響機關信譽以及衍生更多之賠償。

(三)若個資事件影響層面過大，依個人資料保護法施行細則第二十二條但書規定，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通知。通知內容準用前款後段規定。

(四)公開說明注意事項：第一時間應公開相關資訊，並說明機關查明個資安全事故後，依個人資料保護法第二十八條負損害賠償責任。

(五)所有提到之通報行為，機關皆必須留下可資證明之紀錄或證據，如不幸發生訴訟時，亦可取出向法官證明機關確實並非故意造成個資事件，且有誠意解決問題並負起一切責任，降低對機關各種有形或無形之傷害。

(六)若事件後續處理有需要持續觀察或矯正、預防措施需要更長時間者，機關應指派專人進行全程之追蹤、記錄、監控並進行必要之審查，以確保所有控管事項均被完整執行。

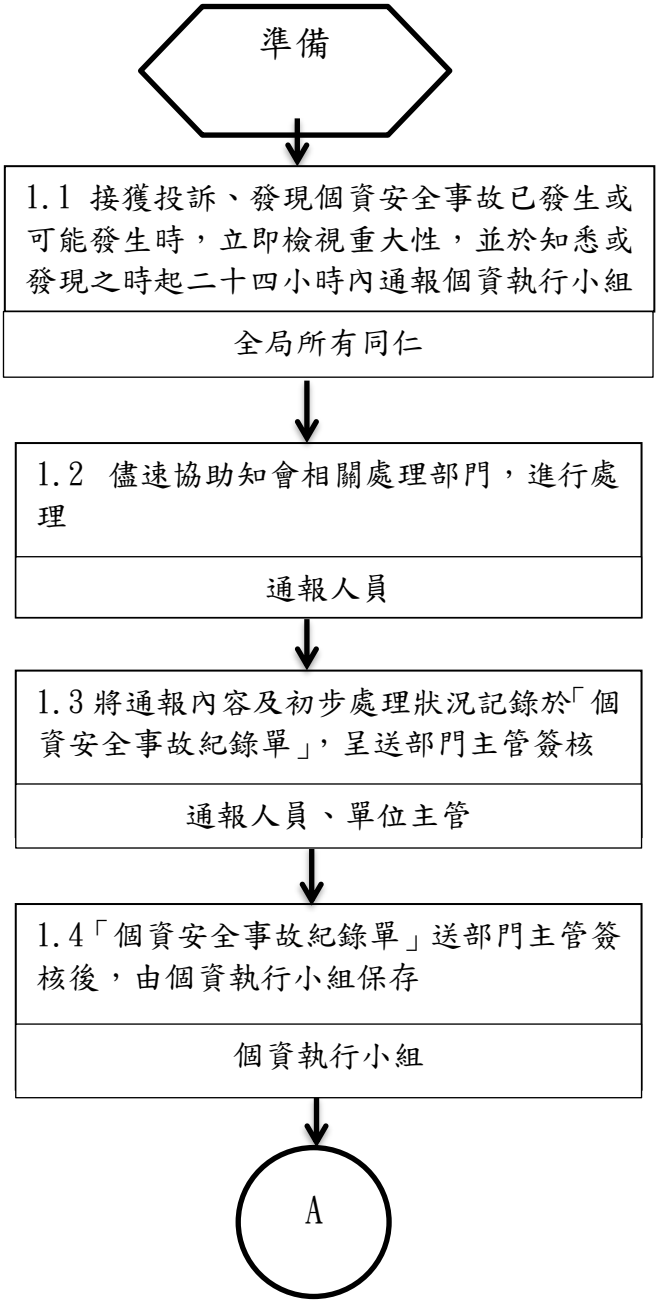
(七)若事件處理時間較長，機關需確保受影響之個資當事人會持續接收機關之處理進度報告。

六、檢討改進

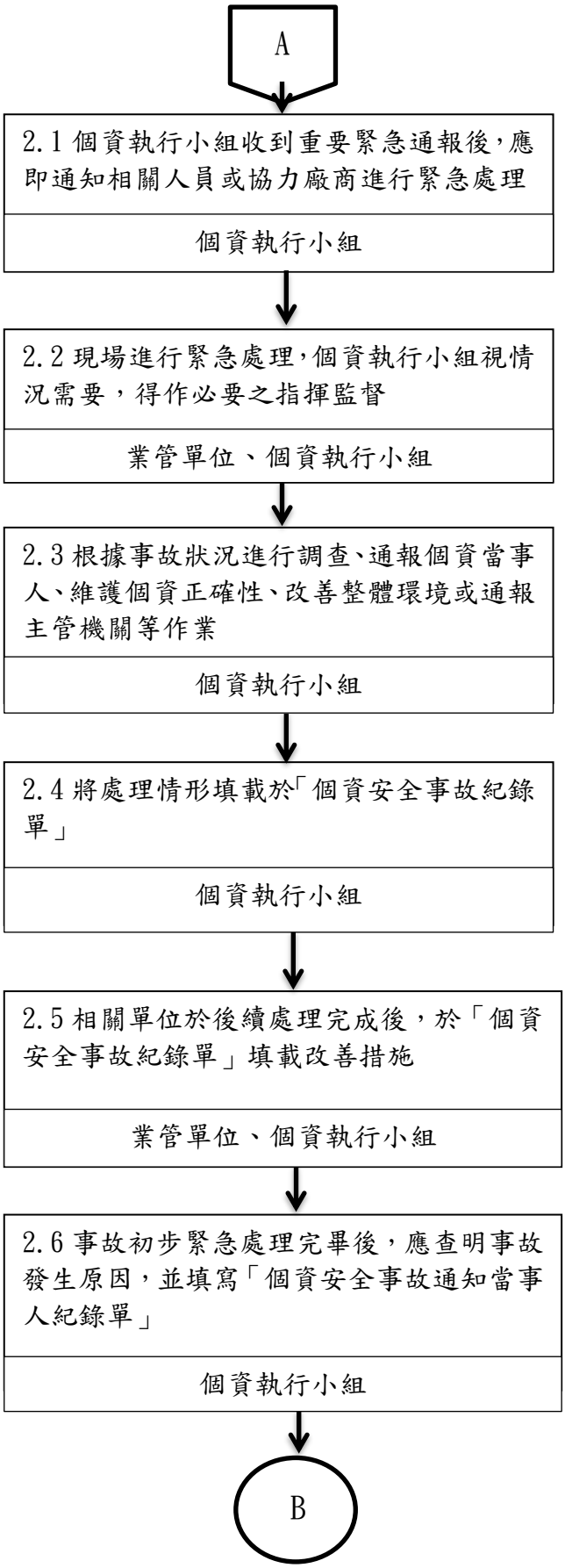
(一)個資事件處理另為確保不再發生錯誤，必須進行後續管理機制的檢討改進。

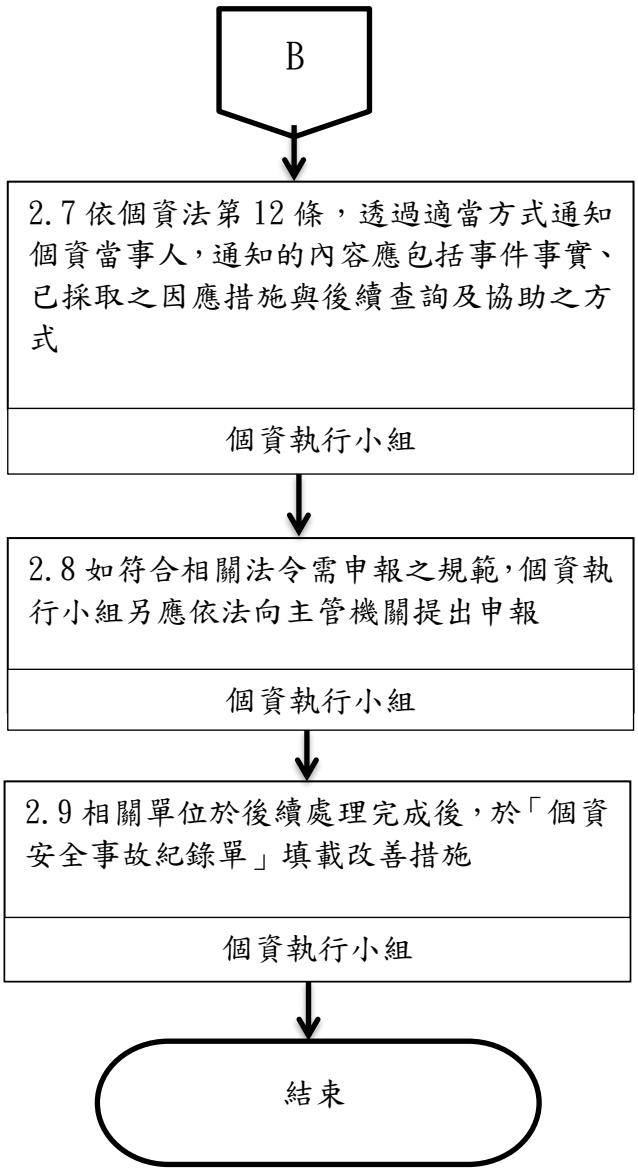
(二)個資安全事故之改善、預防措施及事故發生單位應列為內部稽核作業之重要查核範圍，並辦理追蹤考核。如發現不允當，應要求受查核單位立即改正，並報備個資執行小組。

附圖一、個資安全事故之通報程序



附圖二、 個資安全事故之緊急處理程序




B
2.7 依個資法第 12 條，透過適當方式通知個資當事人，通知的內容應包括事件事實、已採取之因應措施與後續查詢及協助之方式
個資執行小組
2.8 如符合相關法令需申報之規範，個資執行小組另應依法向主管機關提出申報
個資執行小組
2.9 相關單位於後續處理完成後，於「個資安全事故紀錄單」填載改善措施
個資執行小組
結束

附表一：國家科學及技術委員會新竹科學園區管理局個資安全事故紀錄單

填表日期：　　年　　月　　日

一、通報來源、通報事項(接獲通報人填寫)					
單位		姓名		分機	
發生時間	年　　月　　日　　時　　分				
投訴內容 (簡述事件發生經過、內容)	當事人通訊方式　　發生日期： 姓名：　　聯繫方式：				
二、個資安全事件（權責單位填寫）					
事件影響等級	□3 級(高)	□2 級(中)	□1 級(低)		
	等級判定請參考註 5 說明。				
事件類別	□遭竊取或洩露　□資料遭竄改　□檔案毀損或滅失 □違法蒐集處理　□違法利用　□其他				
三、處理措施說明(權責單位簡述處理經過及結果)					
□已通知當事人					
承辦人		單位主管			
會辦單位 (秘書室)					
主任秘書		副局長		局長	

※註：

1. 如為不予以處理之情況，權責單位應將上述告知證據留存至少一年，並通知當事人不處理的原因。
2. 若有伺服器與網路作業稽核軌跡及相關證據應以適當方法保護，以作為未來研析問題之依據。
3. 若已曉得事件發生原因，應迅速進行處置，抑制事件對當事人之損害。
4. 此表單請於完成後，交至秘書室留存紀錄。
5. 事件影響等級判定準則如下：
   (1) 3 級(高)：鉅量個資，數量超過 2000 筆、具 5 個欄位以上之個人資料(資料很詳細)、具任一欄之特種個人資料
   (2) 2 級(中)：大量個資，數量 200~2000 筆
   (3) 1 級(低)：少量個資，數量不足 200 筆

6.權責單位於處理時發現有刑事罪嫌疑者，應向偵查機關告發。

附表二：國家科學及技術委員會新竹科學園區管理局個資安全事故通知當事人紀錄單

通知日期		通知部門/人員	
個資安全事件發生日期			
通知內容	個資被侵害之事實：		
	已採取之因應措施：		

受通知當事人	通知方式