

臺北市政府環境保護局環保稽查大隊

個資事故應變計畫標準作業流程

一、個資事故應變作為分述如下：

(一)個資事故確認階段

發現疑似與個資外洩有關的異常癥兆時，發現異常人員應立即通報直屬主管，並由直屬主管通知發生異常之單位主管及該單位個資專責人員，依所獲知之事實性資訊，及時研判是否構成個資事故，包含個資機密性、完整性、可得性等侵害，並由該單位個資專責人員視需要邀請相關人員共同進行調查，以了解該異常發生之原因並分析判斷是否為個資事故。

(二)個資事故調查、處理階段

- 1、如判斷非為個資事故，發生異常單位仍應採取處理措施並負責持續監控，直到該異常解除或排除。
- 2、如判斷為個資事故，個資事故發生單位應及時啟動緊急應變程序並召開緊急應變會議，研判事故發生之原因與嚴重性，包含評估以下現況與進行初步調查：
 - (1)事故發生來源與原因。
 - (2)確認侵害範圍及影響。
 - (3)事故原因初步分析。
 - (4)可能個資外洩管道。
 - (5)可採取應變措施。
 - (6)所需協助應變之支援。
 - (7)估算回復正常所需時間。
 - (8)事故損害情況。
- 3、個資事故發生單位應依指示及視事件性質，經初步調查後儘

速採取包含下列內容之緊急處置應變措施：

- (1)中斷入侵或洩漏途徑。
- (2)緊急儲存尚未被破壞資料。
- (3)啟動備援程序或替代方案。
- (4)評估受侵害個人資料類別及數量。
- (5)檢視防護及監測設施功能。
- (6)記錄事故經過。
- (7)行政內部調查完成前保存相關證據。
- (8)解決或修復方案。
- (9)通知保有相同資料組室或其他單位。
- (10)若涉及刑事責任者，移請檢警鑑識或調查。

(三)個資事故外部應對

個資事故發生單位應針對個資事故發生進行外部應對包含以下措施：

- 1、個資事故發生後，各單位應儘速完成通報作業。通報對象包括首長及單位主管；通報內容至少應包括通報人身分、資料外洩或侵害方式、時間、地點、初估外洩或侵害個人資料類別及數量、避免損害擴大處置等資訊；通報方式以電話或簡訊為主，電子郵件為輔。重大資通安全事件通報及應變作業，應依資通安全事件通報及應變辦法、臺北市政府資安事件通報及應變管理程序辦理。
- 2、個資事件發生後，應通知當事人，針對當事人個資侵害通知，得以言詞、電話、書面、電子郵件、簡訊、網路、新聞稿或其他足以使當事人知悉或可得知悉之方式為之等。
- 3、外部監督應對，包含適時發布新聞稿、追蹤媒體報導、擬定機關詢問等之回應方案。

(四)個資事故原因檢討及根本原因分析

個資事故發生單位應針對個資事故發生進行原因檢討及根本原因分析包含以下措施：

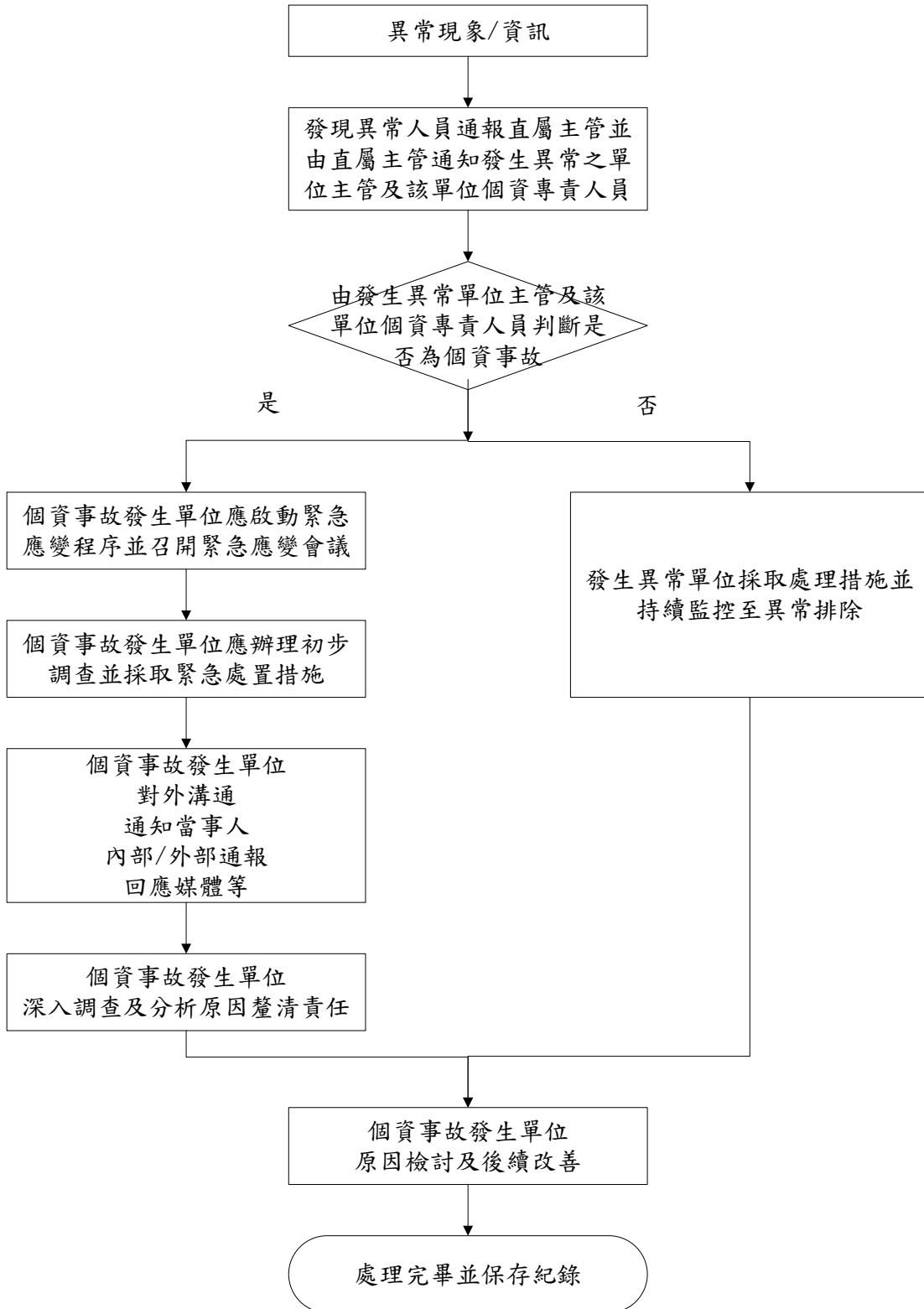
- 1、分析事故發生原因及檢討改善方案。
- 2、提出防止類似事件再次發生之具體方案。

(五)個資事故後續改善作為

清查類似個資漏洞或缺失以修補漏洞，強化防護及監測措施。

二、個資事故發生單位，應依「個資事故應變標準作業流程圖」辦理並填寫「個資事故應變標準作業流程表」以供查核。

個資事故應變標準作業流程圖



臺北市政府環境保護局環保稽查大隊
個資事故應變標準作業流程表

事故描述			
內部回報流程			
事故應變組織			
應變階段		主責單位	因應措施/配合單位
事故應變	初步調查/ 緊急措施		
	對外溝通 (通報)		

	當事人溝通 與協助		
	深入調查/ 原因分析		
	原因檢討/ 後續改善		
追蹤事項			