臺北市政府警察局刑事警察大隊個資事故應變標準作業流程

114 年 11 月 24 日核定

一、依據：

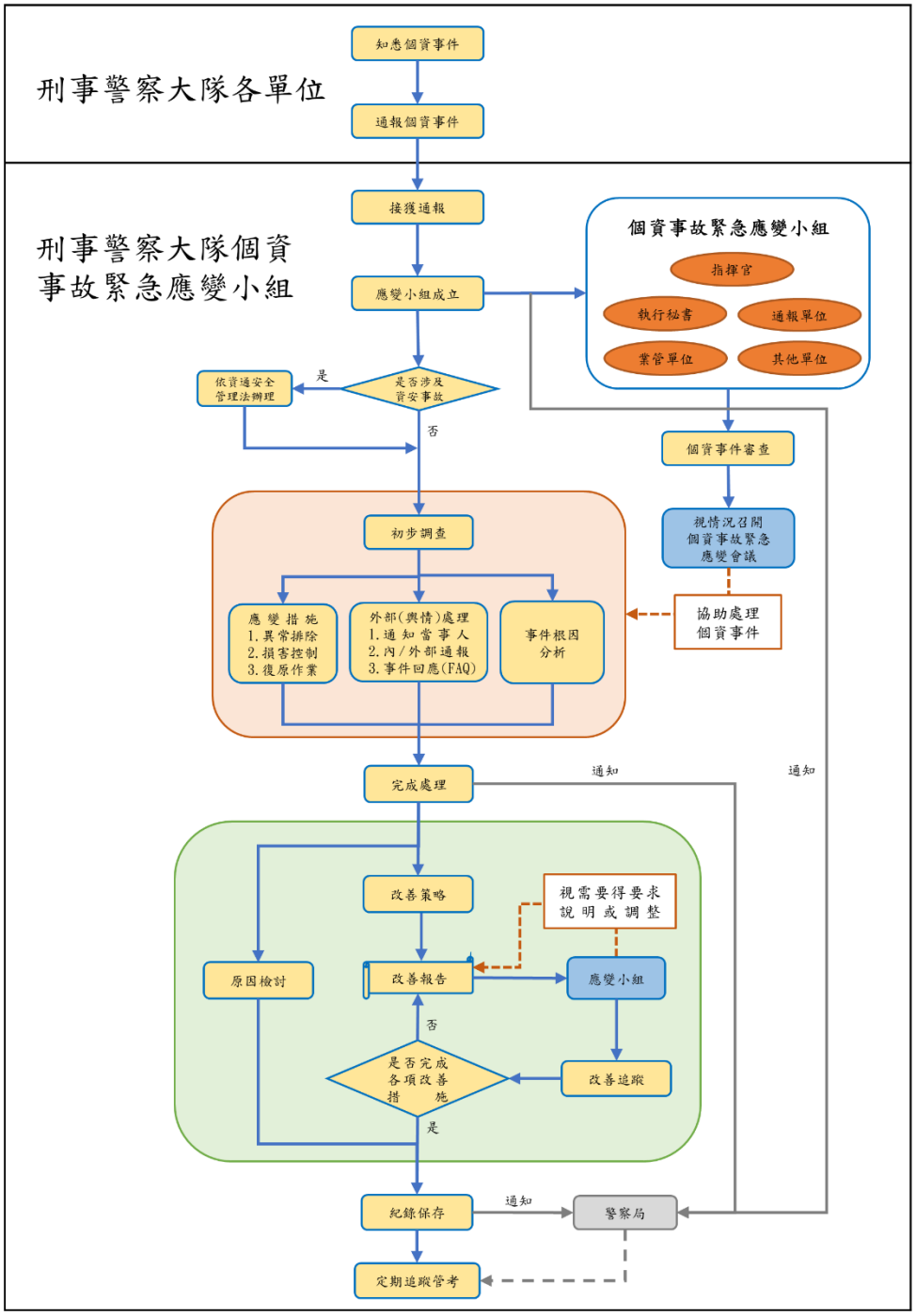
(一)個人資料保護法

(二)個人資料保護法施行細則

(三)臺北市政府資通安全事件通報及應變作業指引

(四)臺北市政府警察局刑事警察大隊個人資料保護管理要點

二、處理流程：



三、注意事項：

(一)準備作業：

1. 依據「個人資料保護法」、「個人資料保護法施行細則」、「臺北市政府資通安全事件通報及應變作業指引」、「臺北市政府警察局刑事警察大隊個人資料保護管理要點」辦理。
2. 成立個資事故緊急應變小組(以下簡稱應變小組)：依前述法規內容組成，分別為指揮官(業管副大隊長)、執行秘書(業管單位主管)、事故通報單位、業務單位及其他相關單位，惟應變小組得依案件性質、影響範圍及專業需求，適時調整成員配置。
3. 個人資料保護聯絡窗口：由業管單位負責受理通報及主導本流程；各單位須配置一名連絡窗口以利進行通報程序。
4. 個人資料盤點：各單位應定期執行個人資料盤點作業及個人資料檔案清冊，以利事故發生時能快速管理及調查分析。

(二)通報作業：

1. 個資事件通知來源：
   (1) 公務機關通報/民間漏洞通報/廠商通知/媒體報導/民眾投訴/網際網路。
   (2) 單位自行發現：網路搜尋/內部設備偵測/稽核檢查/內部控管。
   (3) 其他管道。
2. 確認個資事件類型:依據現況判斷個資事件是否為資安事件,若符合資安事件者,須同步依「資通安全管理法」、「資通安全事件通報及應變辦法」及「修正各機關資通安全事件通報及應變處理作業程序」程序辦理。
3. 踐行個資事故通報程序：
   (1) 各單位應依本大隊個人資料保護管理要點，於知悉個資事件後一小時內，由發現個資事故單位(個人資料保護聯絡窗口)通報應變小組連絡窗口;如認該事件之影響涉及其他單位或應由其他單位依其業務權責處理時,權責人員或應變小組應同步知悉相關單位。
   (2) 各單位需於一小時之內完成通報程序，通報方式以電話或簡訊為主，電子郵件為輔，並於通報後二小時內填寫「個資事故通報單」後回報應變小組。
   (3) 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。
4. 成立應變小組：各單位於完成通報作業後，應變小組立即成立並進行初步損害控制，由應變小組協調各項工作內容，協調形式不拘，就下列事項進行討論：
   (1) 個資事故概況。
   (2) 評估受影響範圍。
   (3) 緊急優先處理事項。
   (4) 其他必要之討論事項。

   若應變小組接獲通報後，如發現情節重大時，得隨即召開個資事故緊急應變會議，由指揮官進行人力、資源上之調配，會議形式及討論內容同應變小組

各項工作。

個資事件得視情形請警察局出席。

5. 各單位個資事故發生時，除依上述規定通報外，應於成立應變小組時，另以電話或其他適當方式通知警察局個人資料保護聯絡窗口。

(三)應變措施：

個資事件發生時，單位應依指示及視事件性質，儘速採取下列措施：

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. 事件原因初步分析(人、事、時、地、物五大面向調查)。
5. 評估受侵害個人資料類別及數量。
6. 檢視防護及監測設施功能。
7. 記錄事件經過。
8. 行政內部調查完成前保存相關證據。
9. 解決或修復方案(恢復正常作業)。
10. 通知保有相同資料組室或其他單位。
11. 洽商專業人員協助或進駐處理(外部協助)。
12. 涉及刑事責任者，移請權管單位依法調查。
13. 發布新聞稿、網站公告。

(四)外部(輿情)處理：

1. 個資事件發生後，本大隊應依本法第十二條通知當事人，內容包括侵害事實及因應措施說明、建議當事人處理事項、提供查詢及協助管道、賠（補）償當事人處理事務相關費用等補救措施。

   前項通知，指以言詞、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。
2. 內/外部通報：依本大隊個資保護管理要點通報，若構成資通安全事件，依資通安全法通報；若個資事件涉及或影響其他單位時，或為避免發生二次事故，將可能之事故原因及初步控制措施提供予相關單位，以及時防堵個資外洩。
3. 事件回應(FAQ)：
   (1) 輿情處理(視情況辦理)：依據新聞輿情進行危機處理及對外公告事件之內容，適時發布新聞稿，追蹤並回應媒體；並擬定議員或上級主觀機關詢問之回應方案。
   (2) 通知當事人內容(視情況辦理)：由應變小組(或會議)內由指揮官協調各小組分工項目。

(五)事件根因分析：

1. 事件完整調查與內部責任釐清：
   (1) 事件發生原因、過程深入調查。
   (2) 確認侵害範圍及影響。

(3) 緊急因應措施有效性初步評估。

(4) 分析內部制度、流程、系統是否有缺失或漏洞。

(5) 釐清內部人員是否有疏失。

2. 依據事件調查報告、處理及改善報告，單位應分析事故原因並提出防止事件再次發生之具體改善方案。

(六)個資事故事件調查、處理及改善報告應包括以下項目：

1. 事故發生、完成損害控制或復原作業之時間。
2. 事故影響之範圍及損害評估。
3. 損害控制及復原作業之歷程。
4. 事故調查及處理作業之歷程。
5. 為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。
6. 前款措施之預定完成時程及成效追蹤機制。

(七)改善措施及追蹤：

1. 進行事件改善追蹤時，須辦理下列事宜：

(1) 檢視改善策略之可行性。

(2) 評估執行成效，以調整改善策略。

(3) 配合上級機關辦理相關改善作為。

2. 相關事故報告、改善措施等內容，需有紀錄並作成報告，格式不拘。
3. 依應變小組(或會議)決議或其他方式，將相關改善事項納入追蹤管考。

(八)紀錄保存：將事故發生始末完整紀錄，除其他法令另有規定或契約另有約定外，應至少保存五年。