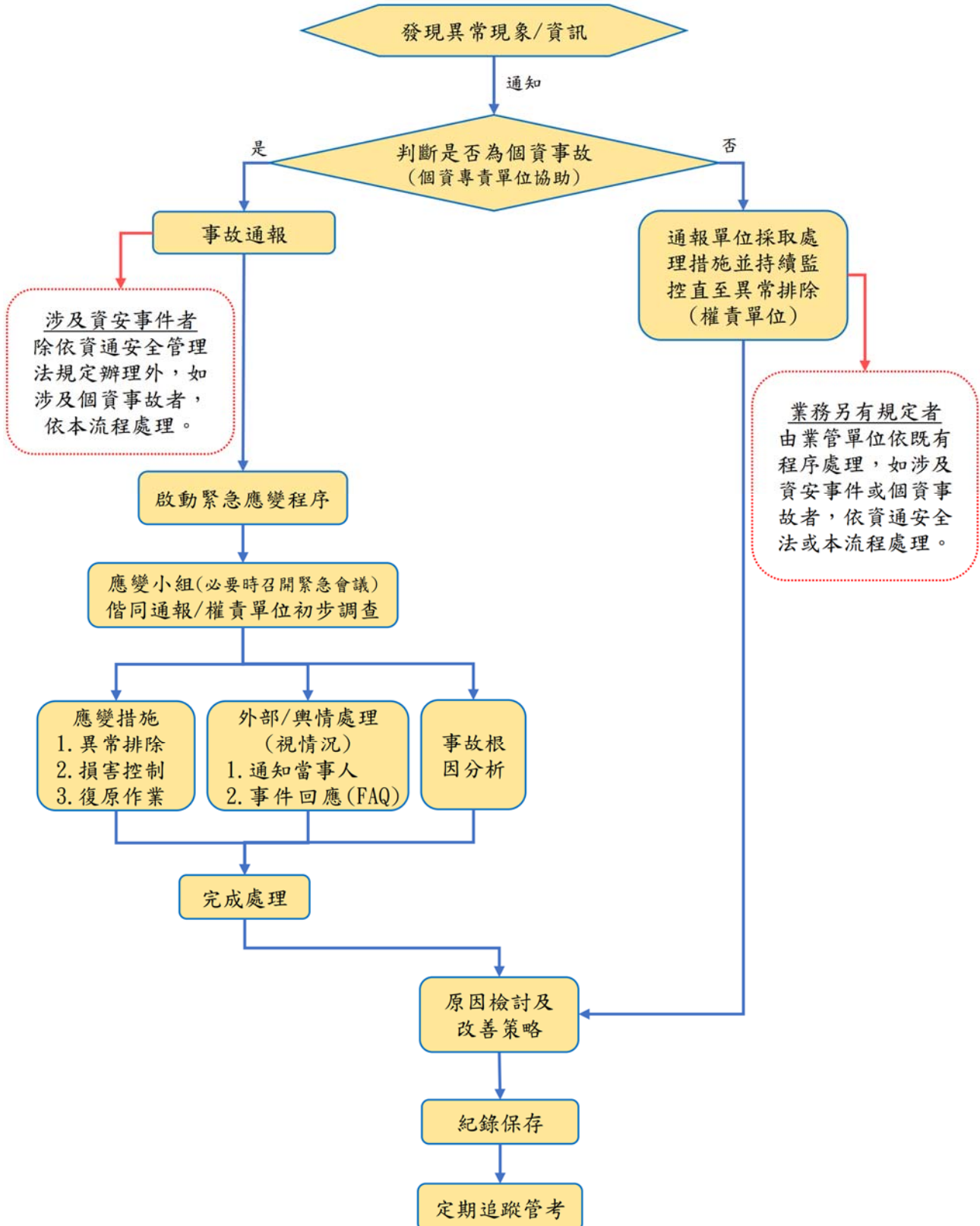


臺北市政府警察局捷運警察隊個資事故應變標準作業流程

112年2月16日核定

一、作業流程圖：



二、依據：

- (一)個人資料保護法(以下簡稱本法)
- (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)臺北市政府警察局捷運警察隊個人資料保護管理要點(以下簡稱本要點)

三、定義及適用範圍：

- (一)個資事故係指違反本法規定，致所處理之個人資料被竊取、竄改、毀損、滅失或洩漏等情事，致侵害當事人權利者為限。(參照本法第 18、28 條)
- (二)涉及資安事件者，應優先依「資通安全管理法」、「資通安全事件通報及應變辦法」、「修正各機關資通安全事件通報及應變處理作業程序」及「臺北市政府資通安全事件通報及應變作業指引」等規定辦理。
- (三)若為異常/不當查詢(例如：定期/不定期之各項稽核或業務內容所為之查核)未達個資事故程度者，由各業管單位依既有程序處理，無須通知個資保護窗口及個資保護專責單位。若後續執行業務時發現有疑似為個資事故，或無法依既有流程繼續進行者，再依本應變處理流程進行。

四、先期作業：

- (一)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，分別為應變小組指揮官(副隊長)、執行秘書(業管單位主管)、事故通報單位、業管單位及其他相關單位(例如：行政組-公關處理、督察組-政風風紀、刑事組-刑案偵查)等，並於發生個資事故時組成應變小組，並視情況由指揮官召開個資事故緊急應變會議(以下簡稱應變會議)。
- (二)個人資料保護聯絡窗口：臺北市政府警察局捷運警察隊(以下簡稱本隊)業管單位同為個資保護專責單位，負責受理通報及主導應變流程；各單位須配置一名聯絡窗口以利進行通知(或通報)程序。

五、作業程序：

- (一)事故來源：
 - 1. 單位自行發現：網路搜尋/內部設備偵測/稽核檢查/內部控管。
 - 2. 公務機關通報/民間通知/廠商通知/媒體報導/民眾投訴/網路/其他。
- (二)異常通知：
 - 1. 各單位人員發現若有異常現象/資訊/個資外洩者，通知該單位個資保護聯絡窗口及其主管，並由個資保護聯絡窗口通知本隊個資保護專責人員。
 - 2. 本隊個資保護專責人員偕同通知單位，初步判斷是否為個資事故，非屬個資事故者由原通知單位持續監控至異常排除。
- (三)通報作業：判斷為個資事故者，應依本要點第四十五點規定於一小時內通報個資保護專責單位，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。
- (四)應變程序：
 - 1. 成立應變小組：事故通報後隨即成立，進行初步損害控制及協調各項工作內容，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。
2. 如情節重大時，得隨即召開應變會議，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。
 3. 應變措施：依本要點第四十三點，儘速採取相關應變措施。
 4. 外部(輿情)處理：
 - (1) 通知當事人(視情況辦理)：依本法第十二條及本要點第四十四點辦理。
 - (2) 事件回應(FAQ)：視情況根據輿情進行危機處理及對外公告相關內容，適時發布新聞稿，追蹤並回應媒體；並擬定上級主管或其他機關詢問之應答方案。
 5. 事故根因分析：針對事故之人(責任釐清)、事(發生原因)、時(發生時間)、地(侵害範圍及影響)、物(損害內容)五大面向進行調查，並對於緊急應變措施進行有效性評估，及提出防範類似事件再次發生之措施等事項。
 6. 相關調查報告、原因檢討及改善策略等內容，需有紀錄。
 7. 追蹤管考：依應變小組(或會議)決議或其他方式，納入定期追蹤管考。
 8. 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，應依本要點第三十九點規定至少保存五年。



臺北市政府警察局捷運警察隊

Rapid Transit Division, Taipei City Police Department R.O.C

個資事故通報單					
事故通報單位聯絡資料					
通報人		單位名稱			
電話		電子郵件			
事故通報事項					
事故發生時間	__年__月__日__時__分		填報日期	__年__月__日__時__分	
事故樣態	<input type="checkbox"/> 個人資料事件 <input type="checkbox"/> 資通安全事件 <input type="checkbox"/> 重大緊急事件 <input type="checkbox"/> 其他事件_____			管制編號	
(應變小組填寫)					
事故簡要說明					
個資事故	等級	第1級	第2級	第3級	第4級
事件等級表	個資筆數	500 以下(含)	501-5000	5001-50000	50000 以上(不含)
事故等級判定	<input type="checkbox"/> 1級 <input type="checkbox"/> 2級 <input type="checkbox"/> 3級 <input type="checkbox"/> 4級 <input type="checkbox"/> 通報警察局				
破壞(外洩)程度	<input type="checkbox"/> 服務中斷 <input type="checkbox"/> 資料庫毀損 <input type="checkbox"/> 資料遭竊取及竄改 <input type="checkbox"/> 系統當機 <input type="checkbox"/> 軟硬體故障 <input type="checkbox"/> 病毒感染 <input type="checkbox"/> 個資被竊取、竄改、毀損、滅失或洩漏 <input type="checkbox"/> 其他_____				
外洩或侵害個人資料類別及數量	<input type="checkbox"/> 類別： <input type="checkbox"/> 數量：				
事故影響範圍及損失評估					
損害控制及復原作業之歷程					
業務服務終止紀錄(必填)	<input type="checkbox"/> 業務維持運作，無須終止服務。 <input type="checkbox"/> 業務需終止服務(起迄時間：__年__月__日__時__分～__年__月__日__時__分)， 總停止服務時間：__日__時__分。				
期望支援項目					
事故調查及處理作業之歷程					
完成損害控制或復原作業之時間	__年__月__日__時__分				
通報單位			個資業管單位		