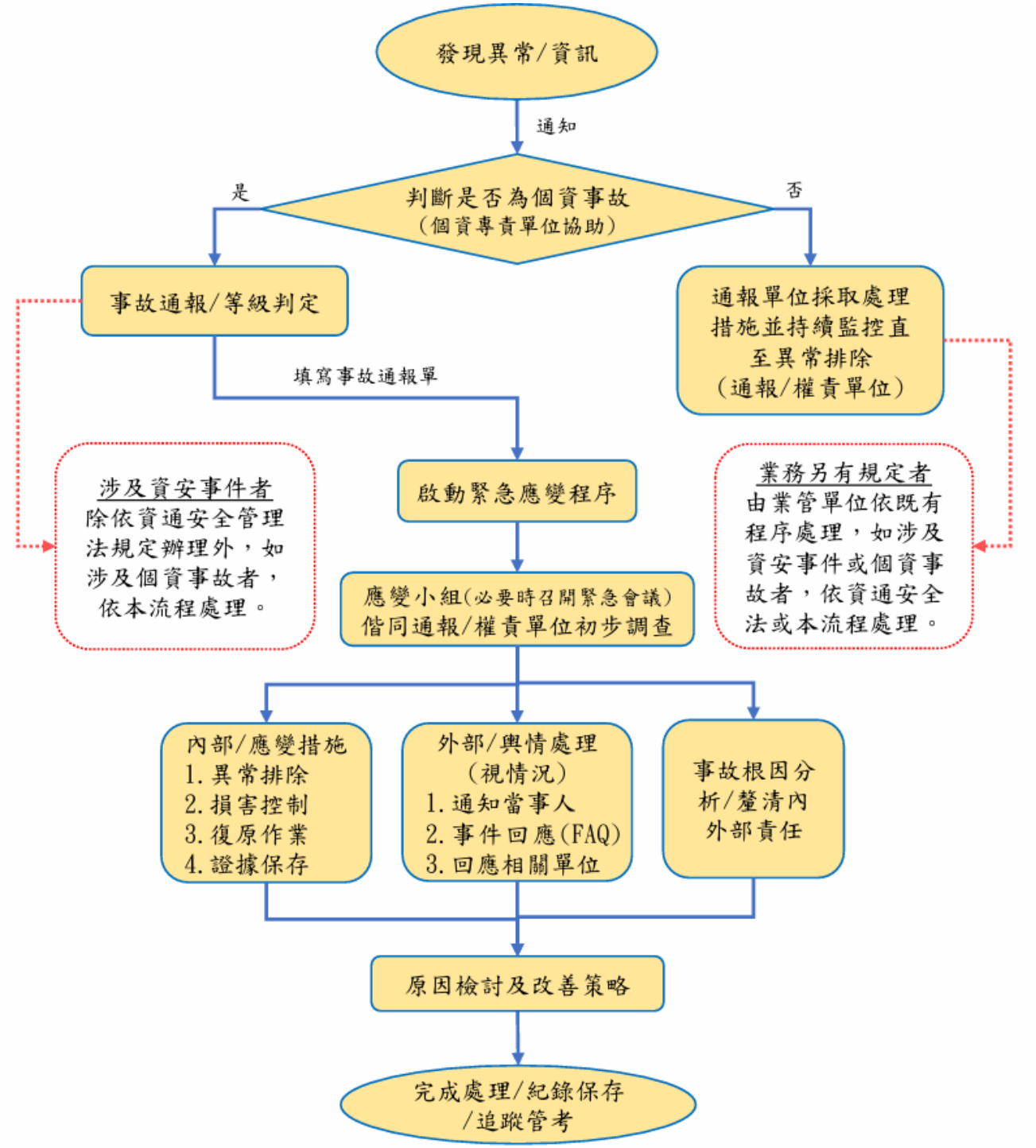
臺北市政府警察局個資事故應變標準作業流程

112 年 2 月 14 日核定
114 年 11 月 19 日修訂

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)發生個資事故時,依臺北市政府警察局個資事故應變標準作業流程(以下簡稱本流程)進行，若於調查過程中發現有涉及資安事件者，應同步依「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,分別為指揮官(主任秘書)、執行秘書(資訊室主任)、事故通報單位、資訊室(業務單位)及其他相關單位(例如：法規室-法治檢核、公關室-輿情處理、政風室-風紀查處)等，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。

(二)個人資料保護聯絡窗口：臺北市政府警察局(以下簡稱本局)業務單位同為個資保護專責單位，負責受理通報及主導本流程；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局個資保護專責人員。
2. 本局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。
3. 若事故來源涉及刑事案件者(如：偵查、偵辦或調查等)，且案件類型明顯與違反本法規定有關者，業管單位應依本流程進行，惟應變小組須注意資料之保護。

(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. 應變小組得視情況，若情節重大時，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。
3. 應變措施：依本要點第四十三點，儘速採取相關措施。
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，並適時紀錄。
7. 追蹤管考：依應變小組(或會議)決議或其他方式，納入追蹤管考。
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
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					
事故知悉時間	___年___月___日___時___分	通報時間 (知悉後1小時內)	___年___月___日___時___分		
填報時間 (通報後2小時內)	___年___月___日___時___分	涉及資通安全事件	□是(資安事件通報) □否	管制編號 (應變小組填寫)	
事故簡要說明	備註：包含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內容。				
事故等級判定及數量	等級	□第1級	□第2級	□第3級	□第4級
	個資筆數	500以下(含)	501-5000	5001-50000	50000以上(不含)
事故個資類別	□一般個資：_____ □特種個資：_____ 備註：如姓名、出生年月日、住址或本法第6條之特種個資等，類別可參考《個人資料保護法之特定目的及個人資料之類別》。				
事故發生種類 (可複選)	□竊取 □竄改 □毀損 □滅失 □洩漏 □其他_____				
初步調查/應變措施/處置歷程 (異常排除、損害控制、復原作業)	備註：配合相關單位進行各式措施，例如：偵查程序、中斷外洩途徑、儲存資料、啟動備援或替代方案、業務流程變動等。				
對外溝通 (公關、輿情處理)	備註：新聞稿、網站公告、追蹤媒體及適時回應或擬相關單位詢問之回應內容。				
當事人通知	方式	□言詞 □書面 □電話 □簡訊 □電子郵件 □傳真 □電子文件 □其他足以使當事人知悉或可得知悉之方式_____			
	內容	備註：通知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。			
事故深入調查/根因分析 (釐清內外部責任)	備註：發生原因、過程、確認侵害範圍、應變措施有效性評估、分析內部制度是否有漏洞疏失或外部責任追究等。				
事故原因檢討/改善策略	備註：提出防止類似事件改善方案及具體措施、制度修補、清查其他可能類似樣態或後續強化作為等。				
其他事項					

通報/權責單位	個資業管單位

機敏資料請勿外洩 1.1