法規名稱：臺北市政府警察局大同分局個人資料保護管理要點
制(訂)定日期：民國 111 年 03 月 28 日
當次沿革：中華民國 111 年 3 月 28 日臺北市政府警察局大同分局（111）北市警同分秘字第1113014346 號函訂定全文 46 點；並自函頒日起生效

柒、個人資料風險評估及安全維護

三十六、電子處理之個人資料安全維護，應遵守資通安全管理法、資通安全管理法施行細則、檔案法、檔案法施行細則、臺北市政府資通安全管理規定、臺北市政府員工使用資通訊裝置應注意事項、臺北市政府及所屬各機關辦理資訊使用管理稽核作業規定、臺北市政府文書處理實施要點等相關法令規定，並得參考行政院國家資通安全會報技術服務中心所訂各項資訊安全參考指引辦理。

非電子處理之個人資料安全維護，應依檔案法、檔案法施行細則、臺北市政府文書處理實施要點、臺北市政府公務機密維護作業等規定辦理。

本分局得因應最新技術發展或資訊安全問題訂定技術指引。

各單位得因應負責業務特性自訂內部安全控制措施或管理細則。

三十七、本分局應規劃並定期執行個人資料盤點作業，作業項目依序如下：

（一）清查各作業流程中所使用之表單、紀錄，並辨識其中與個人資料有關者，歸納整理成個人資料檔案。

（二）使用個人資料盤點表或其他具相同效用之技術、軟體或表單，檢視其保有之個人資料檔案，確認個人資料檔案名稱、保有之依據及特定目的、個人資料種類。

（三）使用個人資料盤點表或其他具相同效用之技術、軟體或表單，檢視其保有之個人資料檔案之生命週期，包含蒐集、處理、利用之內容。

（四）依第一款至前款之檢視結果，建立個人資料檔案清冊。

前項個人資料盤點表及個人資料檔案清冊，包括以下個人資料相關欄位：

（一）所涉主要業務、職掌內容及辦理流程。

（二）個人資料檔案名稱。

（三）業務主管單位。

（四）保存管理單位。

（五）保管方式。

（六）檔案型態，包括紙本類、電子類、可攜式媒體內之電子檔，及系統資料庫。

（七）個人資料來源。

（八）法令或契約上之保有依據。

（九）是否須履行個人資料保護法上之告知義務。

（十）特定目的（依個人資料保護法之特定目的及個人資料之類別填寫）。

（十一）個人資料類別（依個人資料保護法之特定目的及個人資料之類別填寫）。

（十二）個人資料項目。

（十三）個人資料保護法第六條所定個人資料項目。

（十四）個人資料數量。

（十五）內部進行蒐集、處理或利用之單位。

（十六）外部進行蒐集、處理或利用者。

（十七）委外及受委託對象接觸情形。

（十八）法定或自訂之保存期限。

（十九）銷毀方式。

（二十）是否依個人資料保護法第十七條規定對外公告。

（二十一）備註。

三十八、本分局應依前點所定盤點作業結果，規劃並定期執行個人資料風險評估作業，其評估之必要項目如下：

（一）個人資料可識別程度。

（二）個人資料檔案型態及數量。

（三）個人資料類別敏感性及風險性。

（四）蒐集、處理、利用過程及環境。

（五）個人資料存取頻率及存放位置。

（六）蒐集、處理、利用及保有之適法性。

（七）個人資料保護意識及相關知能。

本分局應依前項所定風險評估結果，規劃並採取必要之風險控管及精進措施。

三十九、各單位應視業務性質保存下列紀錄或證據：

（一）當事人書面同意。

（二）告知或通知當事人。

（三）當事人或法定代理人依本法第十條或第十一條第一項至第四項定主張權利。

（四）蒐集、處理、利用個人資料所生之軌跡紀錄（ log）。

（五）依第十六點第一項規定作成之紀錄。

（六）本分局或各單位之檢查或稽核。

（七）依第三十五點規定作成之監督紀錄。

（八）個人資料正確性有爭議。

（九）個資事件。

依前項規定保存之紀錄或證據，除其他法令另有規定或契約另有約定外，應至少保存五年。

四十、為妥善因應個資事件，各單位平時應建立通報及支援聯絡網人員名冊，掌握個人資料處理或利用流程，透過監測資料注意異常狀況之潛在問題。

四十一、負責蒐集、處理或利用個人資料之職員工，應定期參加資訊安全或個人資料保護教育訓練。

新進職員工或參與本分局招標第一次得標廠商員工，應詳閱本要點、相關契約內容，得標廠商亦應提供必要之教育訓練。

專人應適時通知個人資料保護注意事項，並應視需要轉知業務往來之其他機關或單位。

四十二、本分局每年應依臺北市政府資通安全管理規定、臺北市政府及所屬各機關辦理資訊使用管理稽核作業規定辦理相關稽核作業。

四十三、個資事件發生時，單位應依指示及視事件性質，儘速採取包含下

列內容之應變措施：

（一）中斷入侵或洩漏途徑。

（二）緊急儲存尚未被破壞資料。

（三）啟動備援程序或替代方案。

（四）事件原因初步分析。

（五）評估受侵害個人資料類別及數量。

（六）檢視防護及監測設施功能。

（七）記錄事件經過。

（八）行政內部調查完成前保存相關證據。

（九）解決或修復方案。

（十）通知保有相同資料組室或其他單位。

（十一）洽商專業人員協助或進駐處理。

（十二）涉及刑事責任者，移請檢警鑑識或調查。

（十三）發布新聞稿、網站公告。

四十四、個資事件發生後，本分局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。

四十五、個資事件發生後，各單位應儘速於知悉後一小時內完成通報本分局作業。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、臺北市政府資通安全事件通報及應變管理程序辦理。