法規名稱：臺北自來水事業處工程總隊個人資料保護管理要點

制(訂)定日期：民國 111 年 03 月 31 日

當次沿革：中華民國 111 年 3 月 31 日臺北自來水事業處工程總隊奉首長核定以電子郵件下達訂定全文 47 點

壹、總則

一、臺北自來水事業處工程總隊（以下簡稱本總隊）為落實個人資料蒐集、處理或利用法令、尊重當事人資訊自決權、促進個人資料合理利用及避免人格權受侵害，特依個人資料保護法（以下簡稱本法）、個人資料保護法施行細則（以下簡稱本法施行細則）及其他相關法令規定，訂定本總隊個人資料保護管理要點（以下簡稱本要點）。

二、本要點名詞，定義如下：

（一）各單位專人：各單位個人資料保護聯絡窗口。

（二）所屬人員：本總隊執行業務之過程必須接觸個人資料之人員。

（三）幕僚單位：負責本總隊個資保護制度推動、會議聯繫協調及資料綜整等事項之單位。

三、本要點適用於本總隊及受本總隊委託或與本總隊共同蒐集、處理或利用個人資料之其他公務機關或非公務機關。但其他法令另有規定者，從其規定。

貳、個人資料保護管理組織

四、為落實個人資料之保護及管理，得由機關首長指定幕僚單位邀集各單位主管舉行會議審議下列事項：

（一）個人資料保護政策之擬議。

（二）個人資料管理制度之推展。

（三）個人資料隱私風險之評估及管理。

（四）各單位專人與所屬人員之個人資料保護意識提升及教育訓練計畫之擬議。

（五）個人資料管理制度基礎設施之評估。

（六）個人資料管理制度適法性與合宜性之檢視、審議及評估。

（七）其他個人資料保護、管理之規劃及執行事項。

前項會議，得視情形要求各單位專人列席。

五、各單位專人應辦理下列事項：

（一）辦理當事人依本法第十條及第十一條第一項至第四項所定請求事項之考核。

（二）辦理本法第十一條第五項及第十二條所定通知事項之考核。

（三）本法第十七條所定公開或供公眾查閱。

（四）本法第十八條所定個人資料檔案安全維護。

（五）依第四點第四款所為擬議之執行。

（六）個人資料保護法令之諮詢。

（七）個人資料保護事項之協調聯繫。

（八）單位內個人資料損害預防及危機處理應變之通報。

（九）個人資料保護之自行查核及本總隊個人資料保護政策之執行。

（十）其他單位內個人資料保護管理之規劃及執行。

（十一）公務機關間個人資料保護業務之協調聯繫及緊急應變通報。

（十二）個人資料被竊取、洩漏、竄改或其他侵害事件（以下簡稱個資事件）之民眾聯繫單一窗口。

（十三）專人名冊更新。

（十四）專人與所屬人員教育訓練名單及紀錄之彙整。

參、個人資料之蒐集、處理或利用之內部管理程序

六、本總隊應依本要點訂定個資檔案安全維護計畫，以落實個資檔案之安全維護及管理，防止個資被竊取、竄改、毀損、滅失或洩漏。

個資檔案安全維護計畫應包括下列事項：

（一）以合理安全之方式，於特定目的範圍內，蒐集、處理及利用個資。

（二）以可期待之合理安全水準技術保護所蒐集、處理、利用之個資檔案。

（三）設置聯絡窗口，供個資當事人行使其個資相關權利或提出相關申訴與諮詢。

（四）規劃緊急應變程序，以處理個資被竊取、竄改、毀損、滅失或洩漏等事故。

（五）如委託蒐集、處理及利用個資者，應妥善監督受託人。

（六）持續維運本計畫之義務，以確保個資檔案之安全。

七、各單位蒐集、處理或利用個人資料，其類別、數量及接觸人員，應符合本法第五條比例原則，以處理法定職務必要範圍內為限，儘量以蒐集最少且不含本法第六條所定個人資料為原則。

各單位蒐集、處理或利用個人資料之特定目的，以本總隊已依適當方

式公開者為限。有變更者，亦同。

八、各單位蒐集當事人個人資料時，應明確告知當事人本法第八條第一項所列事項。但符合本法第八條第二項規定情形之一者，不在此限。

各單位蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及本法第八條第一項第一款至第五款所列事項。但符合本法第九條第二項第一款至第四款規定情形之一者，不在此限。

依前二項規定為告知，其告知事項內容應使用通俗、簡淺易懂之語文，避免使用艱深費解之詞彙。

依第一項及第二項規定為告知，如有委託或共同蒐集、處理或利用個人資料，應同時告知委託或共同利用情形。

依第一項及第二項規定為告知，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件、明顯或適當處所之公告或其他足以使當事人知悉或可得知悉之方式為之。

九、各單位依本法第六條第一項第六款、第十一條第二項但書或第三項但書規定，經當事人書面同意者，應取得當事人同意之書面文件；該書面文件作成之方式，依電子簽章法之規定，得以電子文件為之。

各單位依本法第十五條第二款或第十六條但書第七款規定經當事人同意者，應符合本法第七條及本法施行細則第十五條所定之方式。

十、各單位蒐集或處理個人資料應符合下列情形之一，並於蒐集時註明蒐

集之特定目的項目及代號：

（一）依本總隊組織自治條例或本法第十五條第一款及本法施行細則第十條所稱執行法定職務。

（二）經當事人同意。

（三）依法受委託執行職務。

十一、對滿七歲之未成年人蒐集或處理其個人資料，有下列情形之一者，得經未成年人本人同意為之，其他情形應得其法定代理人同意：

（一）依其年齡及身分、日常生活所必需。

（二）純獲法律上利益（純粹取得權利或不負任何義務）。

（三）法定代理人事前允許處分財產或營業。

對未滿七歲之未成年人及受監護或輔助宣告之人蒐集其個人資料，應得其法定代理人同意。

法定代理人基於保護未成年人及受監護或輔助宣告之人之利益，得行使本法第十條或第十一條第一項至第四項規定之權利。

本點關於未成年人保障之未盡事宜，依民法及兒童及少年福利與權益保障法等相關規定辦理。

十二、各單位應優先考慮以去識別化或經遮蔽之個人資料為處理或利用。

十三、任何非原蒐集目的之特定目的外之利用，各單位應確認符合本法第十六條但書規定後始得為之，並將利用歷程作成紀錄。

前項情形，宜審酌個案狀況，規劃當事人選擇不同意或退出同意之

機制。

十四、個人資料檔案屬檔案法所稱檔案者，其申請閱覽、抄錄或複製，應依檔案法、檔案法施行細則及臺北市政府（以下簡稱本府）檔案應用相關規定辦理。

依政府資訊公開法申請公開或提供前項規定以外之政府資訊，如涉及個人資料之特定目的外利用，應審酌是否具有本法第十六條但書及政府資訊公開法第十八條第一項第六款所定情形。

十五、各單位對於個人資料之利用，不得為資料庫之恣意連結，且不得濫用。

十六、各單位就所屬人員應採取下列管理措施：

（一）資訊系統存取權限應以作業所需之最小權限為原則，新進或職務異動人員應視業務需求或所屬執掌進行申請。

（二）避免使用共用帳號，如需使用共用帳號，須具正當理由並經權責單位主管核准。

（三）人員報到時，應使其充分瞭解資通安全之工作責任與要求，並簽署「員工保密切結書」。

十七、各單位應採取下列個資管理措施：

（一）運用電腦及相關設備處理個資時，不得將其儲存於可攜式儲

存媒體。

（二）保有之個資，如有加密或遮蔽之必要，應於蒐集、處理或利用時採取適當之加密或遮蔽機制。

（三）傳輸個資時，應確認資料收受者之正確性。

（四）有備份個資之必要時，應比照原本，依本法規定予以保護。

（五）報廢之伺服器、個人電腦、儲存設備於廢棄、捐贈或轉作其他用途時，應將資料儲存媒體進行格式化或銷毀，並應留存紀錄。

（六）妥善保存認證機制及加密機制中所運用之密碼，如有交付他人之必要，亦應妥善為之。

十八、本總隊應採取下列設備安全管理措施：

（一）存放個資實體檔案之專門區域，原則應設置錄影監視系統、門禁系統等設施，以管制進出使用及防止資料外洩遺失。

（二）電腦機房應設置錄影監視及門禁系統。錄影監視紀錄應至少保存一個月。

十九、本總隊應採取適當技術管理措施規範各單位利用電腦或相關設備蒐集、處理或利用個資。

二十、本總隊保有之個人資料有誤或缺漏時，應由資料蒐集單位更正或補充之。

因可歸責於本總隊之事由，未為更正或補充之個人資料，應於更正

或補充後，由資料蒐集單位以通知書通知曾提供利用之對象。

二十一、個人資料正確性有爭議者，各單位應主動或依當事人之請求停止處理或利用。但因執行職務或業務所需，經註明其爭議或經當事人書面同意者，不在此限。

二十二、各單位應定期查明蒐集或處理個人資料適用法令所訂定之保存期間；其未明定者，視執行業務必要性及合理性，於本總隊年度檔案分類及保存年限表明定，或訂定經告知當事人之合理保存期間。

各單位於所保有個人資料之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

二十三、各單位依本法第十一條第四項規定停止蒐集、處理或利用個人資料者，應視個人資料載體性質適當為之。

二十四、個人資料有補充、更正、停止處理或利用、刪除時，應通知曾利用之其他機關或單位；或與其他機關或單位事先協調及規劃個人資料定期更新機制。

個人資料依規定刪除或停止處理、利用前，應對相關系統或服務作影響評估並妥為因應。

二十五、個人資料之刪除，應檢查是否達到資料無法還原或再組合之程度，並得參考「機關檔案保存年限及銷毀辦法」及本府公務機密維護作業等相關規定辦理。

二十六、各單位將個人資料作國際傳輸前，應確認法令限制及他國（境）對個人資料保護法令要求，並為適當保護措施。

肆、機關間個人資料交換運用之內部管理程序

二十七、本總隊與本府所屬機關（以下簡稱本府其他機關）交換運用個人資料，依本章規定辦理；本章未規定者，適用本要點其他規定。

二十八、本章所稱交換運用，指本總隊為與本府其他機關共同執行法定職務，或協助本府其他機關執行法定職務，而以本府名義蒐集個人資料，並將所蒐集之個人資料提供予各該本府其他機關。

二十九、本總隊為辦理交換運用，應於蒐集個人資料前，確認所涉本府其他機關之法定職務依據、特定目的、需提供之個人資料類別、利用之期間、地區、對象及方式，經簽會本府法務局並簽報本府同意後，始得為之。

前項所定應確認事項，應於蒐集個人資料前，以本府名義明確告

知當事人。但有第七點第一項但書或第二項但書所定情形者，不在此限。

依前二項規定辦理之交換運用，視為本法第二條第四款及本法施行細則第六條第二項所定內部傳送。

伍、當事人權利之行使

三十、當事人依本法第三條、第十條或第十一條第一項至第四項規定向本總隊請求答覆查詢、提供閱覽、製給複製本、更正、補充、停止蒐集、處理、利用或刪除個人資料時，應經身分確認程序，本總隊並得視情形請當事人檢附相關證明文件或為適當之釋明。

第三十九點所定紀錄或證據，視為前項個人資料。

第一項證明文件內容如有遺漏、欠缺或釋明不完整，應通知限期補正。

申請案件有下列情形之一者，應以書面或電子文件駁回其申請：

（一）申請文件內容有遺漏、欠缺、虛偽不實或釋明不完整，經通知限期補正，逾期仍未補正或無法補正。

（二）有本法第十條但書各款情形之一。

（三）有本法第十一條第二項但書或第三項但書所定情形之一。

（四）與法令規定不符。

第一項請求之處理期限及延長，依本法第十三條規定辦理。

三十一、當事人請求閱覽、抄錄或複製個人資料，得依檔案閱覽抄錄複製收費標準收取費用。

前項情形，由各單位派員陪同為之。

三十二、各單位提供當事人閱覽、抄錄或複製個人資料前，應確認未同時揭露他人個人資料。

三十三、本總隊保有個人資料檔案以公開於機關網站之個人資料保護專區為原則，並應於建立個人資料檔案後一個月內為之；更新檔案時，亦同。

為確保當事人有充分表達意見機會及申訴管道，本總隊網站之個人資料保護專區，應設有個人資料客訴聯絡方式。

陸、委外監督

三十四、各單位研擬業務委外招標文件時，應就委外範圍擬定投標廠商須具備個人資料保護管理能力，於招標文件訂定評選項目或於採購契約訂定監督事項及罰則條款，並將本要點列入採購契約文件供廠商遵循。

三十五、契約終止、解除或屆滿時，廠商應返還或刪除所保有之個人資料，或交接本總隊指定之其他單位，刪除存取權限，並切結未以任何形式保留備份或影本；續約廠商不在此限。

履約期間廠商員工離職或留職停薪，應說明所負責系統之存取權限及完成鎖定帳號或停止系統權限之時點，並應更換離職或留職停薪員工曾接觸之密碼。

三十六、各單位於履約期間應定期確認廠商執行個人資料保護措施並予以記錄。

柒、個人資料風險評估及安全維護

三十七、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、本府資通安全管理規定、本府員工使用資通訊裝置應注意事項、本府及所屬各機關辦理資訊使用管理稽核作業規定、本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、本府文書處理實施要點、本府公務機密維護作業等規定辦理。

本總隊得因應最新技術發展或資訊安全問題訂定技術指引。

本總隊因應各單位業務特性得訂定內部安全控制措施或管理細則。

三十八、本總隊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）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。

三十九、本總隊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。

本總隊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。

四十、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）依第十二點第一項規定作成之紀錄。

（六）本總隊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。

四十一、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。

四十二、負責蒐集、處理或利用個人資料之所屬人員，應定期參加資訊安全及個人資料保護教育訓練。

新進所屬人員或參與本總隊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。

各單位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。

四十三、本總隊每年應依本府資通安全管理規定、本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。

四十四、個資事件發生時，各單位應依指示及視事件性質，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。

四十五、個資事件發生後，本總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。

四十六、個資事件發生後，各單位應依本總隊個資事件通報流程完成通報作業。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、本府資通安全事件通報及應變管理程序辦理。

捌、附則

四十七、本總隊為因應法令修訂、技術發展或強化人格權保障，應為必要之補充及調整，並適時修正本要點。