自來水事業個人資料檔案安全維護計畫標準辦法

中華民國102年10月30日經水字第10204802900號令訂定

中華民國105年4月1日經水字第10504601260號令修正第十七條

第一條　本辦法依個人資料保護法（以下簡稱本法）第二十七條第二項及第三項規定訂定之。

第二條　自來水事業，其用戶數在五千戶以上者，應依本辦法規定訂定個人資料檔案安全維護計畫（以下簡稱本計畫），以落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

第三條　本辦法用詞定義如下：

一、個人資料管理代表：由自來水事業代表人擔任，或由代表人直接授權，負責督導本計畫之規劃、訂定、執行、修訂及相關決策之人員。

二、所屬人員：執行業務之過程必須接觸個人資料之人員。

第四條　自來水事業應建立個人資料檔案安全維護管理組織，並配置相當資源，負責本計畫相關程序之規劃、訂定、執行及修訂等任務。

個人資料管理代表非由自來水事業代表人擔任時，應定期就個人資料檔案安全維護管理組織執行任務情形，向自來水事業代表人提出書面報告。

第五條　自來水事業應依其組織與事業特性訂定個人資料保護管理政策，提報自來水事業代表人核定，並公開周知，使其所屬人員均明確瞭解及遵循。

前項管理政策至少應包括下列事項之說明：

一、遵守我國個人資料保護相關法令規定。

二、以合理安全之方式，於特定目的範圍內，蒐集、處理及利用個人資料。

三、以可期待之合理安全水準技術保護其所蒐集、處理、利用之個人資料檔案。

四、設置聯絡窗口，供個人資料當事人行使其個人資料相關權利或提出相關申訴與諮詢。

五、規劃緊急應變程序，以處理個人資料被竊取、竄改、毀損、滅失或洩漏

等事故。

六、如委託蒐集、處理及利用個人資料者，應妥善監督受託人。

七、持續維運本計畫之義務，以確保個人資料檔案之安全。

第六條　自來水事業應定期檢視應遵循之個人資料保護法令，並據以訂定或修訂本計畫。

第七條　自來水事業為確保個人資料之蒐集符合個人資料保護相關法令要求，應就下列事項建立相關程序：

一、檢視蒐集個人資料之特定目的及法定要件。

二、檢視具備法令所要求之特定情形或其他要件。

第八條　自來水事業為遵守本法第八條及第九條有關蒐集個人資料之告知義務規定，應就下列事項建立相關程序：

一、檢視蒐集、處理個人資料之特定目的。

二、檢視是否符合免告知之事由。

三、除屬免告知者外，應依據資料蒐集之情況，採取適當之告知方式。

第九條　自來水事業為確認對個人資料之利用，符合個人資料保護相關法令，應就下列事項建立相關程序：

一、檢視個人資料之利用符合特定目的。

二、檢視是否得進行及如何進行特定目的外利用。

第十條　自來水事業新增或變更特定目的時，應依下列程序為之：

一、依第八條規定之告知程序辦理。

二、取得當事人書面同意。但法令另有規定者，不在此限。

第十一條　自來水事業就本法第六條之特種個人資料，應就下列事項建立相關程序：

一、檢視其蒐集、處理及利用之個人資料是否包含特種個人資料及其特定目的。

二、檢視其蒐集、處理及利用特種個人資料，是否符合相關法令規定。

第十二條　自來水事業為提供當事人行使本法第三條規定之權利時，應就下列事項建立相關程序：

一、提供當事人行使權利之方式。

二、確認當事人身分。

三、確認有無本法第十條及第十一條得拒絕當事人行使權利之情況。

四、遵守本法第十三條有關處理期限之規定。

五、訂定酌收必要成本費用之標準。

第十三條　自來水事業為維護其保有個人資料之正確性，宜採取下列方法：

一、檢視個人資料於蒐集、處理及利用過程，是否正確。

二、當檢視資料有不正確時，應適時更正或補充。

三、定期檢查資料之正確性。

個人資料正確性有爭議者，自來水事業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。

因可歸責於自來水事業之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用對象。

第十四條　自來水事業於所保有個人資料之特定目的消失或期限屆滿時，應遵守本法第十一條第三項規定。

第十五條　自來水事業應依個人資料保護法令，定期清查所保有之個人資料，界定其納入本計畫之範圍並建立清冊，且定期確認其變動情形。

第十六條　自來水事業應依前條界定之個人資料範圍及其相關業務流程，分析可能產生之風險，並依據風險分析結果，訂定適當管控措施。

第十七條　自來水事業為因應其保有之個人資料被竊取、竄改、毀損、滅失或洩漏等事故，應就下列事項建立相關程序：

一、採取適當之應變措施，以降低或控制事故對當事人之損害，並通報有關單位。。

二、查明事故之狀況並適時通知當事人事故之事實、所為之因應措施及諮詢服務專線等內容。

三、研議預防機制，避免類似事故再次發生。

四、致危及正常營運或大量當事人權益時，應立即以電話、傳真、發函或其他書面方式通知中央自來水主管機關。

第十八條　自來水事業應採取下列人員管理措施：

一、指定蒐集、處理及利用個人資料個別作業（以下簡稱作業）流程之負責人員。

二、就個別作業設定所屬人員不同之權限並控管之，以一定認證機制管理其權限，且定期確認權限內容設定之適當與必要性。

三、要求所屬人員相關之保密義務。

第十九條　自來水事業應採取下列資料管理措施：

一、運用電腦及相關設備處理個人資料時，應訂定使用可攜式儲存媒體之規範。

二、保有之個人資料，如有加密之必要，應於蒐集、處理或利用時採取適當之加密機制。

三、傳輸個人資料時，應確認資料收受者之正確性。

四、有備份個人資料之必要時，應比照原本，依本法規定予以保護。

五、儲存個人資料之媒介物於廢棄或轉作其他用途時，應採取適當防範措施。

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。

第二十條　自來水事業應採取下列設備安全管理措施：

一、依作業內容之不同，實施適宜之進出管制。

二、妥善保管個人資料之儲存媒介物。

三、針對不同作業環境，審酌建置必要之防護設備或技術。

第二十一條　自來水事業利用電腦或相關設備蒐集、處理或利用個人資料時，應採取下列技術管理措施：

一、於電腦、相關設備或系統上設定認證機制，對有存取個人資料權

限之人員進行識別與控管。

二、認證機制使用帳號及密碼之方式時，應具備一定安全之複雜度並定期更換密碼。

三、於電腦、相關設備或系統上設定警示與相關反應機制，以對不正常之存取為適當之反應與處理。

四、對於存取個人資料之終端機進行身分認證，以識別並控管之。

五、個人資料存取權限之數量及範圍，於作業必要之限度內設定之，且原則上不得共用存取權限。

六、採用防火牆或路由器等設定，避免儲存個人資料之系統遭受無權限之存取。

七、使用可存取個人資料之應用程式時，應確認使用者具備使用權限。

八、定期測試權限認證機制之有效性。

九、定期檢視個人資料之存取權限設定正當與否。

十、於處理個人資料之電腦系統中安裝防毒軟體，並定期更新病毒碼。

十一、對於電腦作業系統及相關應用程式之漏洞，定期安裝修補之程式。

十二、定期瞭解惡意程式之威脅，並確認安裝防毒軟體及修補程式後之電腦系統之穩定性。

十三、具備存取權限之終端機不得安裝檔案分享軟體。

十四、測試處理個人資料之資訊系統時，不使用真實之個人資料，如使用真實之個人資料時，應明確規定其使用之程序。

十五、處理個人資料之資訊系統有變更時，應確認其安全性並未降低。

十六、定期檢查處理個人資料資訊系統之使用狀況及個人資料存取之情形。

第二十二條　自來水事業應定期對所屬人員施以認知宣導及教育訓練，使其明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。

第二十三條　自來水事業為確保本計畫之有效性，應定期稽核本計畫是否落實執行。

第二十四條　為持續改善本計畫，自來水事業應建立下列程序：

一、本計畫發生未落實執行時之改善程序。

二、本計畫有變更時之變更程序。

第二十五條　本計畫各項程序執行時，自來水事業至少應保存下列紀錄：

一、個人資料使用紀錄、留存自動化機器設備之軌跡資料之紀錄或相關證據保存紀錄。

二、檢視個人資料正確性及更正之紀錄。

三、提供當事人行使權利之紀錄。

四、個人資料刪除、廢棄之紀錄。

五、存取個人資料系統之紀錄。

六、備份及還原測試之紀錄。

七、所屬人員權限新增、變動及刪除之紀錄。

八、所屬人員違反權限行為之紀錄。

九、因應事故發生所採取行為之紀錄。

十、定期檢查處理個人資料之資訊系統之紀錄。

十一、教育訓練之紀錄。

十二、本計畫稽核及改善程序執行之紀錄。

第二十六條　業務終止後個人資料處理方法得採下列方式為之，並留存下列紀錄：

一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。

三、其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

第二十七條　本辦法自發布日施行。