水利署臺北水源特定區管理分署
防火牆管理作業標準書

V2.0

文件編號	WRATB-ISMS-3-003
分類等級	內部使用
初版日期	
修訂日期	

制訂	審查	會辦	核准

文件編修紀錄

發行／修訂版本	發行／修訂生效日期	發行/修訂內容說明	制訂	審查	核准	備註
V1.0		規範防火牆設備管理作業，制定本作業標準書。		資通安全執行秘書	資通安全處理小組召集人	
V2.0		機關 112 年 9 月組織改造後名稱修正、內文、分類修訂		資通安全執行秘書	資通安全處理小組召集人	

目錄

0. 目的

為保護水利署臺北水源特定區管理分署(以下稱本分署)內部各電腦主機、網路設備之安全與正常運作，提供防火牆系統日常作業及設備管理之規範。

1. 範圍

本分署網路防火牆之安全管理。

2. 相關文件

無。

3. 作業說明

3.1 名詞定義

無。

3.2 角色與權責

3.2.1 權責主管

3.2.1.1 核准「WRATB-ISMS-4-042 防火牆安全控管規則設定申請單」。

3.2.2 防火牆管理人員

3.2.2.1 填寫「WRATB-ISMS-4-042 防火牆安全控管規則設定申請單」。

3.2.2.2 進行防火牆規則清查，填寫「WRATB -ISMS-4-041 防火牆規則清查紀錄表」。

3.2.2.3 執行防火牆規則及系統的異動。

3.2.2.4 執行防火牆日誌管理。

3.3 防火牆系統設置原則

3.3.1 應透過防火牆機制，區隔網路（Intranet）、非軍事武裝區 （DMZ）與網際網路（Internet）；並應將提供公開服務之主機（網站主機、郵件主機等）建置於非軍事武

裝區 （DMZ）；除特殊因素外，來自於網際網路之連線將僅允許其連接至本分署非軍事武裝區 （DMZ）之主機。

3.3.2 防火牆應開啟適當稽核功能，記錄連線狀況。

3.3.3 本分署防火牆之取存政策採正面表列方式進行控管。

3.3.4 重要主機須經由防火牆控管，只開放本分署內部使用者及內部非軍事武裝區伺服器進入，並只開放業務所需之必要服務通道，禁止由網際網路直接進入擷取資訊。

3.3.5 除特殊狀況與業務需求外，須指定來自網際網路連線之網路位置（IP），方可連線至位於非軍事武裝區提供業務必要服務之主機。

3.3.6 對外開放之各業務網站、電子郵件，防火牆應開放其所需之服務通道，例如 HTTP、HTTPS，其餘非相關之服務通道一律禁止通行，並拒絕非軍事武裝區主機主動連線至網際網路。

3.3.7 除網際網路區使用外部公共（開）IP 外，由防火牆系統隔開之內部區域網路均設定為虛擬私有 IP，以阻絕公眾由網際網路直接進入內部各區域網路存取資源；對外開放公眾由網際網路進入之伺服器（如：網站伺服器），應由防火牆系統轉址為外部公共（開）IP。

3.4 防火牆設定異動

3.4.1 防火牆異動執行前，須備份原有設定檔或記錄原有設定值。

3.4.2 防火牆安全規則的新增、異動或刪除，防火牆管理員應填寫「WRATB-ISMS-4-042 防火牆安全控管規則設定申請單」，並經權責主管同意後方能進行。

3.4.3 當有防火牆系統修正程式發佈時，防火牆管理人員應進行評估後，在不影響本分署業務正常營運之前提下進行更新，必要時得協同委外廠商進行防火牆系統評估及更新作業。

3.5 防火牆系統管理

3.5.1 本分署的防火牆系統管理，除內部許可之 IP 可使用加密方式（如 SSL）連接登入管理外，其餘 IP 一概不得登入防火牆系統，亦不可使用撥接網路（Dial- up Connection）或網際網路，由外部網路遠端管理本分署的防火牆系統。

3.5.2 為避免防火牆系統規則及參數設定因時間或業務變更等相關因素導致產生不符合現狀之處，防火牆管理人員應每年重新檢討規則及參數設定之適當性，並填寫「WRATB-ISMS-4-041 防火牆規則清查紀錄表」，由各業務科室主管覆核後，據以修正防火牆規則。

3.5.3 防火牆管理人員應適當保留防火牆設備所產生之日誌，應每月定期予以檢視，並保留至少 6 個月。

4. 產出紀錄

4.1 WRATB-ISMS-4-041 防火牆規則清查紀錄表

4.2 WRATB-ISMS-4-042 防火牆安全控管規則設定申請單