水利署臺北水源特定區管理分署
資訊存取控制程序書

V2.0

文件編號	WRATB-ISMS-2-009
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		為確保本局資通系統之存取權限規範，建立本程序書初稿。		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

為管控水利署臺北水源特定區管理分署(以下稱本分署)各項資訊作業可以有效率執行、避免非經授權之存取，進而防範任何有意或無意之資訊洩漏或竄改，以維持資訊作業正常運作，特制定本程序書。

1. 範圍

本分署提報之核心資通系統及重要系統之資訊存取控管。

2. 相關文件

2.1 經濟部水利署及所屬資通安全事件通報及應變程序

3. 作業說明

3.1 名詞定義

3.1.1 惡意軟體:意指意圖攻擊或入侵使用者電腦、主機或網路設備的軟體程式，包含電腦病毒、網路蠕蟲、特洛伊木馬、後門程式和邏輯炸彈等。

3.1.2 手動資料交換或傳輸:係指不透由網路，藉由可攜式讀寫儲存媒體（包括可讀寫光碟片、USB 儲存媒體、快閃記憶體、磁帶、可攜式硬碟及磁片等）或可攜式設備（如筆記型電腦、掌上型電腦及 PDA 等）來進行資料交換或傳輸。

3.2 角色與權責

3.2.1 權責科室主管

3.2.1.1 核准使用科室填寫之「WRATB-ISMS-4-026 網管作業配合職務申請表」。

3.2.1.2 核准使用科室填寫之「WRATB-ISMS-4-027 帳號權限異動申請表」。

3.2.1.3 核准系統管理員填寫之「WRATB-ISMS-4-028 存取權限審查表」。

3.2.1.4 核准安全性更新作業。

3.2.1.5 核准弱點掃瞄作業及「WRATB-ISMS-4-029 弱點處理通知單」。

3.2.1.6 核准事件紀錄的調閱。

3.2.1.7 核准與交付外部機關的資料。

3.2.2 使用科室

3.2.2.1 填寫「WRATB-ISMS-4-026 網管作業配合職務申請表」，提出網域、各作業系統及各資通系統之帳號申請、使用者離/調職帳號刪除申請。

3.2.2.2 填寫「WRATB-ISMS-4-027 帳號權限異動申請表」，提出特殊權限、委外廠商或臨時聘僱人員帳號申請。

3.2.3 系統管理員

3.2.3.1 系統管理員填寫「WRATB-ISMS-4-028 存取權限審查表」，進行存取權限審查。

3.2.3.2 進行安全性更新作業。

3.2.3.3 進行弱點掃描及修補作業，並填寫「WRATB-ISMS-4-029 弱點處理通知單」。

3.2.3.4 管理及審查事件紀錄。

3.2.3.5 對於核心資通系統及重要系統，執行備份檔案的還原演練作業。

3.2.4 企劃科科長

3.2.4.1 指派可攜式設備及媒體管理人。

3.2.4.2 核准「WRATB-ISMS-4-024 電腦設備連網使用申請表」。

3.2.5 企劃科

3.2.5.1 管理病毒碼更新狀態，處理電腦中毒事件。

3.3 使用者帳號及權限管理

3.3.1 帳號及密碼管理

3.3.1.1 有關本分署使用者網域、各資通系統等之使用者帳號申請、異動，使用科室應填列「WRATB-ISMS-4-026 網管作業配合職務申請表」辦理（有關水利署網域、各資通系統之使用者帳號申請、異動，請依據水利署相關流程申請）。

3.3.1.2 非本分署人員（委外廠商或臨時聘僱人員等）之帳號，應透過「WRATB-ISMS-4-027 帳號權限異動申請表」申辦，待該專案或工作結束，由

系統管理員進行帳號停用及刪除設定作業。

3.3.1.3 使用者均有獨立的帳號與密碼，不允許與他人共用。

3.3.1.4 **密碼的設定應符合下列原則**：

3.3.1.4.1 **使用者於初次登錄時，應強迫其立即變更密碼**。

3.3.1.4.2 密碼長度不可少於 **12** 個字元。

3.3.1.4.3 密碼至少每 **90 天**更改一次，並不得與前 3 次相同。

3.3.1.4.4 密碼應為**英數字**及**特殊字元**混合設定。

3.3.1.4.5 若該資訊設備無法以強制方式進行上述之設定或自動執行變更，應告知提醒使用者自行依規定變更。

3.3.1.4.6 **特殊權限**之密碼應符合下列原則：

3.3.1.4.6.1 密碼應有專人管理。

3.3.1.4.6.2 密碼長度不可少於 15 個字元。

3.3.1.4.6.3 密碼至少每 30 天更改一次，並不得與前 3 次相同。

3.3.1.4.6.4 密碼應為英數字及特殊字元混合設定。

3.3.2 權限管理

3.3.2.1 使用特殊權限帳號之人員，平時一般工作應有其他帳號使用，特殊權限帳號之使用僅限於經授權核准之事項。

3.3.2.2 特殊權限之帳戶，需填寫「WRATB-ISMS-4-027 帳號權限異動申請表」，並經權責科室主管授權後辦理。

3.3.3 使用者存取權限的審查

3.3.3.1 各項資通系統帳號及權限，包含特殊權限帳號，應定期審查帳號權責是否相符。

3.3.3.2 執行帳號權限審查時，系統管理員填寫「WRATB-ISMS-4-028 存取權限審查表」後，送權責主管進行審核。

3.4 安全性更新及弱點掃描與處理

3.4.1 安全性更新

3.4.1.1 系統管理員應隨時蒐集並訂閱來自國家資通安全會報技服中心、軟硬體系統廠商、安全方案廠商等所發布之技術弱點知識或攻擊警訊，以確保收到弱點及相關安全性更新的通知。

3.4.1.2 系統管理員於收到弱點及相關安全性更新的通知後，應進行評估或測試作業，經評估需要進行修補或更新作業時，需要取得權責主管的同意才進行修補或更新作業。

3.4.1.3 弱點的修補及處理，請參考下列「3.4.3 漏洞修補」及「3.4.4 殘餘弱點之管理作業」之說明。安全性更新，則經權責主管同意後實施，實施紀錄可以保存於日常的維運紀錄或是系統紀錄中。

3.4.2 弱點掃描期程

3.4.2.1 本分署核心資通系統及重要系統應定期執行弱點掃描作業（執行週期依據資通安全法 C 級機關應辦事項辦理）。

3.4.2.2 掃描程式應於掃描前更新至最新模組。

3.4.2.3 掃描結果應依規定發起矯正措施。

3.4.3 漏洞修補

3.4.3.1 弱點修補應視系統重要性先於測試環境測試，運行無礙後再修補；弱點之修補如因設備或預算等因素之限制無法測試者，系統管理員應將相關風險告知權責主管，經同意後執行修補。

3.4.3.2 系統管理員應將弱點掃描修補結果，記錄於「WRATB-ISMS-4-029 弱點處理通知單」，呈交權責主管覆核。

3.4.4 殘餘弱點之管理作業

3.4.4.1 弱點若因故無法成功補強，系統管理員須依據補強作業實際情形說明無法補強的原因、過去曾經發現但仍未補強的歷史紀錄等資訊。

3.4.4.2 弱點處理後，若仍無法將此弱點完全解除，除應紀錄說明原因外，亦應考慮其他積極性預防方式，以降低弱點被攻擊者利用之風險，包括：

3.4.4.2.1 使用廠商所建議之增強式安全性組態避免攻擊。

3.4.4.2.2 加強帳號與密碼的管制。

3.4.4.2.3 加強弱點相關之服務通訊埠管制。

3.4.4.2.4 詳細清查該設備之使用狀況與事件紀錄。

3.4.4.2.5 增加該設備所在環境之防禦設備（含防毒系統、防火牆、入侵偵測或入侵防禦系統等）。

3.4.4.2.6 提升該弱點的風險等級。

3.4.4.2.7 直接考慮軟硬體升級。

3.5 惡意軟體防範

3.5.1 企劃科應定期確認本分署之個人電腦、筆記型電腦、各伺服器均已安裝防毒軟體，並維持正常啟動狀態。

3.5.2 病毒碼需適時保持更新。

3.5.3 使用者不得任意更換本分署預先安裝的防毒軟體。

3.5.4 所有使用者如遇疑似中毒情況，應立刻通報企劃科，由企劃科協助處理，處理結束後應**記錄病毒處理過程**；若為防毒軟體攔截通知，則應確認該病毒已被隔離或刪除，不另記錄。

3.6 可攜式資訊設備(行動裝置)、媒體管理

3.6.1 本分署擁有之可攜式設備及媒體，由**企劃科科長**指定專人管理。

3.6.2 本分署擁有之可攜式資訊設備(智慧型手機與平板電腦)應設定自動鎖定功能，以進行畫面鎖定模式。如以密碼進行畫面解鎖，密碼管理需要符合本分署要求。

3.6.3 非本分署擁有之可攜式設備與媒體若需連結至本分署主機、網路及資通系統時，需填寫「WRATB-ISMS-4-024 電腦設備連網使用申請表」，經企劃科科長核准後，需執行掃毒程式及安全檢查確認安全後才能使用。

3.6.4 只透過無線網路連線之可攜式資訊設備，僅能連接外網，未經同意不得連接本分署內部網路。

3.7 即時通訊軟體管理

3.7.1 利用本分署網路使用即時通訊軟體，應以公務使用為限。

3.7.2 禁止使用即時通訊軟體傳送機敏資料。

3.7.3 為方便公務訊息傳遞之即時性，可建立公務即時通訊群組，以利公務作業。

3.7.4 各公務即時群組應指定管理者，並由管理者統一管理群組人員之加入與退出。

3.7.5 應避免在公用電腦登入個人即時通訊帳號。

3.7.6 即時通訊密碼應定期變更，密碼設定可參考本程序書 3.3.1.3 辦理。

3.7.7 如有需要，應定期進行通訊紀錄之備份並妥善保存。

3.7.8 如發現即時通訊軟體之異常或有惡意訊息之散佈，應立即進行通報與處理。

3.8 手動資料交換或傳輸

3.8.1 手動資料交換應採取彌封或專人遞送等其它具保密機制之傳遞方式，以確保交換資料之機密性、完整性及可用性。

3.8.2 若為機密、敏感性或含有敏感性個人資料(如身分證字號)，其交換或傳送以手動為之的情況下，則可以用具備壓縮通行碼之壓縮軟體為之。

3.8.3 通行碼的產生由資料傳送者為之，通行碼的強度須符合本程序書規範，通行碼知悉人僅可是該壓縮檔之傳送者及指定接收者。

3.8.4 當該壓縮檔傳達到指定的接收者且已透由通行碼解壓後，傳送者得將其擁有的壓縮檔予以刪除，並須當場確認指定接收者所接收到的壓縮檔亦已刪除。

3.8.5 可移動讀寫儲存媒體或可攜式設備不得存有機密、敏感性或含有敏感性個人資料(如身分證字號)及不得存有非經 3.7.3 所處理過的資料。

3.8.6 可移動唯讀儲存媒體(如一般光碟片)不得做為機密、敏感性或含有敏感性個人資料(如身分證字號)的手動資料交換或傳輸的儲存媒介。

3.9 外部機關資料交付管理

3.9.1 資料交付評估

3.9.1.1 本分署與外部機關進行之資訊交換前，應進行下列各項因素的評估，並經權責單位主管核准後才能進行交換：

3.9.1.1.1 存取的目的及用途，是否具備正當性?

3.9.1.1.2 是否合乎法規或主管機關的要求?

3.9.1.1.3 提供該資訊資產之存取是否有其必要性？例如，係基於軟硬體廠商維護之需求、或基於具合作協議關係之要求？

3.9.2 資料交付給外部機關的過程中，須依據交付資料的特性，實施適當的保護機制，避免資料於傳送過程中內容遭毀損或遭外洩。

3.9.3 資料交付後，應取得接收方接收到資料的回覆紀錄。

3.10 電子郵件安全

3.10.1 本分署之電子郵件服務係提供業務上作業所需，禁止同仁發送未經授權之廣告信件、垃圾信件或使用郵件炸彈，並嚴禁任何利用本分署電子郵件進行任何違法行為。其涉有不法行為者，應由當事人自負法律責任，本分署並將主動配合相關機關調查處理。

3.10.2 本分署同仁有義務妥善保管郵件信箱之帳號與密碼，遵循密碼原則設定適當之密碼，並為此組帳號與密碼登入系統後所進行之一切活動負責。

3.10.3 **本分署保留備份所有電子郵件之權利，並在下列情況下允許適當揭露郵件內容**：

3.10.3.1 基於法規或受司法機關或其他有權機關基於法定程序之要求。

3.10.3.2 保障本分署財產及權益。

3.10.3.3 其他使用者或第三人提出合理可信之說明，主張該等電子郵件涉及侵害其名譽、隱私權、智慧財產權或其他權利時。

3.10.4 「機密」等級或含有敏感性個人資料(如身分證字號)之資料或文件，應避免採用電子郵件傳遞，如有必要，應將機密或敏感性資料加密後方可傳送。

3.10.5 電子郵件附件需經掃毒後方可寄出或開啟使用。收到存有病毒之外部郵件及垃圾郵件時，應立即刪除，不可轉寄其他同仁。如收到內部同仁轉寄之病毒或垃圾郵件，應立即通知系統管理人員進行處理。

3.10.6 本分署除正式郵件伺服器外，嚴禁同仁在內部網路未經授權私自架設郵件伺服器；新增主機的 SMTP 服務除非必要，應予以關閉。

3.11 事件紀錄保留與查核

3.11.1 事件紀錄分類

3.11.1.1 資通系統登出、入紀錄:系統使用者登出、入紀錄。

3.11.1.2 資通系統資料存取紀錄:系統使用者讀取資料紀錄。

3.11.1.3 資通系統資料交易紀錄:系統使用者異動資料紀錄。

3.11.1.4 作業系統事件紀錄:如 Windows 作業系統應用程式、安全性、系統紀錄、Unix 作業系統 Syslog 系統紀錄等。

3.11.1.5 資料庫管理者紀錄:資料庫管理者操作資料庫之行為紀錄。

3.11.2 重要系統需產生事件紀錄並遵守以下原則：

3.11.2.1 所有的事件紀錄，包含紙本或電子形式，應加以控管以防止非授權人員的塗改或破壞。

3.11.2.2 所有的相關紀錄，應集中進行控管。

3.11.2.3 事件紀錄之調閱，應取得權責主管的授權，並由系統管理員進行調閱，若調閱作業如係屬廠商執行契約規範，則不在此限。

3.11.3 事件紀錄審查

3.11.3.1 核心資通系統及重要系統之系統管理員應**定期**審查事件紀錄，以評估是否有無違反存取權限的資通安全事件，以維護系統存取安全。

3.11.3.2 如果發現資通安全事件，則應遵循「經濟部水利署及所屬資通安全事件通報及應變程序」之規範要求辦理。

3.12 電腦輸出、輸入作業安全

3.12.1 電腦連線輸入作業安全

3.12.1.1 連線即時處理作業，輸入資料應受連線程式之控制與檢驗。

3.12.1.2 機密資料應被限制只能由特定工作站操作啟動。

3.12.2 電腦輸出作業安全

3.12.2.1 電腦輸出報表、單據等，應按有關規定分別妥善運用、裝訂、保管或逾保存期限後銷毀。

3.12.2.2 對於機密性或含有敏感性個人資料(如身分證字號)之報表，要由專人列印，並放置於非開放式之空間。

3.13 備份作業管理

3.13.1 各科室應考量規劃下列資訊資產的備份作業：

3.13.1.1 資通系統程式原始碼，應定期備份，並保留最新版本。

3.13.1.2 資通系統資料庫。

3.13.1.3 資通系統事件紀錄。

3.13.1.4 資通系統設定及參數檔。

3.13.1.5 科室維運的重要電子檔案。

3.13.2 各科室應依據規劃的備份作業，實施備份活動。

3.13.3 核心資通系統及重要系統之系統管理員應每年定期執行備份作業的還原演練，以確保備份檔案的可用性。

4. 產出紀錄

4.1 WRATB-ISMS-4-026 網管作業配合職務申請表

4.2 WRATB-ISMS-4-027 帳號權限異動申請表

4.3 WRATB-ISMS-4-028 存取權限審查表

4.4 WRATB-ISMS-4-029 弱點處理通知單

4.5 WRATB-ISMS-4-024 電腦設備連網使用申請表