水利署臺北水源特定區管理分署
資通系統安全管理程序書

V2.0

文件編號	WRATB-ISMS-2-010
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		為本局資通系統之開發及維護管理有所依循，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

為使本分署資通系統之開發及維護管理有所依循，維持系統安全與正常運作。

1. 範圍

本分署提報之核心資通系統及重要系統之系統開發與維護。

2. 相關文件

2.1 WRATB-ISMS-2-004 資訊資產管理程序書

2.2 WRATB-ISMS-2-009 資訊存取控制程序書

2.3 WRATB-ISMS-2-015 變更管理作業程序書

2.4 資通安全責任等級分級辦法說明

2.5 水利署及所屬機關資訊相關系統開發與維護注意事項

3. 作業說明

3.1 名詞定義

3.1.1 外購方案：係指向軟體廠商直接購買套裝軟體，包含進行部分客制化修改，但仍維持整個系統之主體架構。

3.1.2 委外資訊服務：係指將資訊需求委外予軟體廠商依據需求進行，包含系統之分析、設計、測試、訓練及輔導上線；承辦人員則參與系統開發、測試、上線及驗收之相關過程。

3.1.3 自行開發方案：係指由本分署自行進行開發、測試及上線。

3.1.4 資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。資通系統可以是外購方案、委外資訊服務或自行開發方案。

3.1.5 資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。

3.1.6 核心服務:本分署依組織法規，足認該資通服務為本分署核心權責所在。

3.1.7 核心資通系統:指支持核心服務持續運作必要之資通系統。

3.2 角色與權責

3.2.1 科室主管

3.2.1.1 指派各資通系統管理員。

3.2.1.2 依據本管理程序書，監督各項執行工作。

3.2.2 資通系統管理員

3.2.2.1 負責資通系統需求分析、規劃、開發、測試、變更及上線作業。

3.2.2.2 管理資通系統程式原始碼。

3.2.2.3 監督委外廠商。

3.2.3 委外廠商

3.2.3.1 遵循本管理程序書及合約規範要求。

3.2.3.2 遵循「水利署及所屬機關資訊相關系統開發與維護注意事項」之作業要求。

3.3 資通系統安全政策

3.3.1 資通系統於系統開發生命週期中，皆應將資通安全需求納入考量。

3.3.2 本分署所有資通系統，需符合「資通安全責任等級分級辦法」之附表十中資通系統防護基準所有控制措施的要求。

3.3.3 資通系統經由委外資訊服務方式時，必須遵循「水利署及所屬機關資訊相關系統開發與維護注意事項」中的要求。

3.4 系統開發生命週期（SDLC）管理

3.4.1 需求分析階段

3.4.1.1 系統開發人員應進行資通系統安全需求分析，評估資通系統當安全控制措施不足時，可能帶來的影響風險。

3.4.1.2 安全需求分析，可以考量下列事項：

3.4.1.2.1 使用者身分認證。

3.4.1.2.2 角色分工與存取權限控制。

3.4.1.2.3 輸入、輸出檢核處理。

3.4.1.2.4 建置事件紀錄，保存資通系統作業紀錄。

3.4.1.2.5 保護機密性或敏感性(如：含有個人資料)資料，防止洩漏或被竄改，必要時應使用資料加密等技術保護。

3.4.1.2.6 具高完整性要求的資料，應在資料處理過程的每一階段，或是特別選定的某一階段，檢查及保護資料之正確性。

3.4.1.2.7 遵守相關法規、契約上對資通安全控制之要求。

3.4.1.2.8 重要的資料應進行備份。

3.4.1.2.9 擬定資通系統的回復作業程序，對高可用性要求的資通系統應評估備援機制。

3.4.1.2.10 保護資通系統避免未經授權的竄改或修改。

3.4.1.2.11 依據資通系統功能，其他需考量的安全控制措施。

3.4.1.3 資通系統於需求分析階段，應保存安全需求分析的相關紀錄，如:需求規格書。

3.4.2 規劃設計階段

3.4.2.1 新資通系統規劃及既有資通系統改版時，應考量加入自動化控制措施（如資料輸入／輸出驗證、錯誤訊息顯示…等），和輔助性控制措施（如系統權限稽查、參數設定…等），來達成需求分析階段的安全需求。

3.4.2.2 資通系統於規劃設計階段，應保存規劃設計的相關紀錄，如: 「設計規格書」。

3.4.3 開發、變更與測試階段

3.4.3.1 開發與測試環境，應與正式維運環境區隔。

3.4.3.2 資通系統經由委外資訊服務方式時，交付廠商之測試資料內容應以必要內容為原則，涉及機密性資料者應予亂碼化。

3.4.3.3 資通系統於測試環境進行測試，除測試系統功能外，亦應測試安全性，如：存取控制強度、系統回復測試、最新弱點驗證及木馬程式檢查…等，若有發現異常狀況，應採取適當的措施進行修補，直到符合安全需求為止。

3.4.3.4 資通系統變更，應遵循「WRATB-ISMS-2-015 變更管理作業程序書」之規範要求。

3.4.3.5 開發或變更完成之資通系統經測試後，確認符合需求後才能上線。

3.4.3.6 資通系統進行測試後，應保存測試之相關紀錄，如:測試過程紀錄、測試報告。

3.4.4 上線階段

3.4.4.1 系統管理人員應於資通系統上線前，規劃上線之相關作業並擬定回復計畫(Back-out Plan)，以避免上線失敗所造成之影響。

3.4.4.2 資通系統上線後應辦理相關教育訓練。

3.4.4.3 若為外購方案之資通系統，應符合以下要求才能上線：

3.4.4.3.1 密碼機制強度應符合本分署要求。

3.4.4.3.2 能明確建立權限劃分設定。

3.4.4.3.3 能提供系統存取、帳號密碼變更的日誌功能。

3.4.4.3.4 通過安全檢測。

3.5 存取控制

3.5.1 資通系統使用者的密碼管理，應遵循「WRATB-ISMS-2-009 資訊存取控制程序書」之規範要求。

3.5.2 資通系統存取其他作業系統或資料庫所使用的帳號，應避免寫入程式中，並應考量資通系統所需使地之權限，應盡量避免直接使用系統最高權限。

3.6 檔案及資料之保護

3.6.1 程式原始碼由資通系統管理員負責管理。

3.6.2 程式原始碼需有**版本管理**，並留存最近新之檔案。

3.6.3 若需使用機敏性測試資料，測試環境之安全管控應比照正式維運環境，對於所使用之測試資料應加以保護。

3.6.4 資通系統的所有相關文件，應遵循「WRATB-ISMS-2-004 資訊資產管理程序書」之規範要求。

4. 產出紀錄

4.1 資通系統開發生命週期之相關紀錄