水利署及所屬機關資訊相關系統開發與維護注意事項

中華民國 95 年 12 月 11 日經水資字第 09512A04406 號函訂定
中華民國 98 年 10 月 19 日經水資字第 09812A03142 號函修訂
中華民國 100 年 06 月 07 日經水資字第 10012A01381 號函修訂
中華民國 100 年 12 月 15 日經水資字第 10012060360 號函修訂
中華民國 103 年 01 月 10 日經水資字第 10312000870 號函修訂
中華民國 104 年 02 月 17 日經水資字第 10412005760 號函修訂
中華民國 105 年 11 月 16 日經水資字第 10512039990 號函修訂
中華民國 110 年 04 月 14 日經水資字第 11012007490 號函修訂

一、為使水利署(以下簡稱本署)及所屬機關之主辦單位、受託廠商於進行各項資訊系統開發與維護時，有效進行資訊安全管制與確保軟體開發及維護品質，特訂定本注意事項。

二、本注意事項依資訊系統開發與維護之生命週期，就系統評估、需求與系統分析、系統設計、程式開發、系統測試、教育訓練、系統上線及系統維護等八階段作說明，但各計畫得依系統開發與維護之需要，自行調整執行順序、跨階段適用相關規定。

三、本注意事項所稱執行單位為實際進行系統開發維護單位，如系統為主辦單位自行開發維護，執行單位為主辦單位；如系統為委外開發維護，執行單位即為受託廠商。委外開發應依政府採購及資通安全相關法規、契約內容及本注意事項辦理。

四、系統評估

(一)起始作業：系統開發需求產生時，主辦單位於起始階段即應對現行作業、系統需求可行性、資訊軟硬體資源、資訊安全防護等加以評估及準備：

1. 所需資訊設備、雲端基礎環境、雲端運算環境、作業管理、資料儲存及查詢、資料供應、大數據及人工智慧運算服務等，應申請使用本署雲端作業平臺所提供之雲端資源及服務，避免重複建置或租用。如有另建主機之需求，主辦單位應簽奉核可後，方可建置。
2. 虛擬主機之安裝軟體（至少含資料庫、作業系統、伺服軟體、文書軟體等），以開源軟體為主，若需使用授權軟體，應於計畫內評估並編列相關經費。
3. 物聯網系統應參考民生公共物聯網計畫資訊安全要求評估規劃資通訊安全管理作業。
4. 資料庫不應重複建置，在建置前應先至本署水利資料整合雲及水資源物聯網感測基礎雲端作業平臺查詢有無相關資料可取用。如有重複建立資料庫之需求，主辦單位應簽奉核可後，方可建置。新建資料庫，應符合政府資料標準平台公告之資料標準及以下規定：
   (1)納入物聯網系統之資料，應依物聯網系統規定辦理。
   (2)涉及流通共享者，應符合水資源資料交換標準，並透過水利資料整合雲或水資源物聯網感測基礎雲端作業平臺進行資料共享與交換。
5. 應參考行政院資通安全處「擴大盤點所使用或採購之大陸廠牌資通訊產品原則」規劃辦理。

(二)計畫書之準備：如為委託服務計畫，主辦單位應依本署委辦計畫管理系統所提供之計畫書格式研擬，且敘明廠商應依本注意事項、資通安全管

理法及其子法執行計畫。

(三)開放資料(Open Data)之研訂及開放：除涉及國家機密、資訊安全、無法去識別化之個人資料及其他依政府資訊公開法第十八條限制公開之資料外，主辦單位應詳實盤點可公開之資料並規劃開放期程，納於計畫工作項目中，落實資料開放政策。

五、需求與系統分析

(一)本階段產出文件為需求規格書，參考格式如附件一。

(二)訪談規劃：執行單位須製作訪談預訂時程表，內容包括：訪談目的與議題、時間、地點、人員、訪談對象需要提供與配合的事項、訪談進行的方式等。

(三)訪談記錄與確認：對需求之確認應填寫系統需求訪談紀錄表(參考格式如附件二)，併入需求規格書附件。

(四)需求規格書注意要項如下：

1.對機密及敏感性資料，應考量建置獨立或專屬作業環境，不得存放於對外開放的資訊或資料庫系統中。

2.應對系統未來容量需求預作規劃分析：

(1)資料量分析 — 預估資料年成長量。

(2)使用者分析 — 主要使用人數、尖峰使用人數、尖峰時段。

(3)網路分析 — 網路流量。

(4)伺服器分析 — CPU、RAM、硬碟容量。

(5)系統相容性分析 — 作業系統、資料庫、既有應用系統、既有第三方套件軟體、既有第三方函式、既有第三方組件、既有介接應用程式，既有提供介接應用程式。

(6)資料相容性分析 — 既有系統內容資料、既有提供其它應用系統介接之資料。

(7)資訊安全防護分析 — 預估資訊應用系統之資訊安全防護所需之機制、功能、設備及人員。

(五)地理資訊之應用系統規劃與建置及地理圖資建置、取得與更新等，應分別 依據水利署及所屬機關地理資訊應用系統規劃建置作業規範、水利署及所屬機關地理資訊圖資管理作業規範辦理。

(六)系統應依據資通安全責任等級分級辦法附表九、資通系統防護需求分級原則進行系統資安等級評估；工業控制系統應依據經濟部能源及水資源領域工業控制系統資安防護基準、其餘資通系統依據資通安全責任等級分級辦法附表十、資通系統防護基準，分別分析規劃系統架構與各項管理政策，及落實於後續各階段執行；如有提供行動化服務，則應依據行政院及所屬各機關行動化服務發展作業原則辦理；本署並得就相關管控措施進行檢核。物聯網系統應參考民生公共物聯網計畫資訊安全要求分析規劃資通訊安全管理作業。

(七)依據「行政院各機關資通安全事件通報及應變處理作業程序」，核心資通系統應保存最近六個月之日誌紀錄，包括作業系統日誌(OS event log)、網站日誌(web log)、應用程式日誌(AP log)及登入日誌(logon log)。

(八)系統如保有個人資料，應設安全管控措施(針對個人資料檔案及資料庫

之儲存，應適當加密；存取時，應提供使用者識別、鑑別及身分驗證管理機制；留存相關日誌紀錄並定期檢視，或設置存取監控之系統化預警機制)，傳遞須採加密方式，離線備份之資料亦應管控，受託廠商於契約終止後應返還、確實刪除或銷毀相關個人資料並保留紀錄。對內系統呈現介面上，如有個資資訊，應評估使用情境，予以適當且一致性之遮蔽隱碼機制，以為個資保護。

(九)系統開發與維護人員使用之電腦設備必須安裝防毒軟體，且病毒碼已更新到最新版本，並設定定期執行全磁碟掃描。

六、系統設計

(一)本階段產出文件為設計規格書，參考格式如附件三。

(二)資料庫除依本注意事項第四點規劃之外，亦應考量安全性、備份機制、容量及效能管理等各面向。

(三)使用者介面設計應與時俱進，依使用者需求及使用裝置、主流瀏覽器、資安要求等調整精進；並應視需要支援跨瀏覽器、響應式設計、視覺化呈現統計數據、提供防呆及線上輔助機制等，以提升使用者體驗。

(四)身分驗證及權限控管：

1.各系統應配合本署所提供之單一簽入機制進行使用者身分驗證及授權：

(1)署內（含所屬機關）同仁使用採本署AD帳號登入。

(2)非本署人員採E政府帳號登入，並以內政部核發之自然人憑證或E政府帳號進行驗證。

2.使用者於各應用系統之權限角色由各系統自行控管，且應採最小權限原則。

(五)應符合「推動ODF-CNS15251為政府文件標準格式」政策。

(六)履約標的涉及共通性應用程式介面開發或整合者，應依國家發展委員會訂定之「共通性應用程式介面規範」辦理。

(七)對外服務網站：

1.網頁目錄架構應妥適規劃、目錄及檔案命名易懂、以相對路徑做鏈結、且應視權限管制需要，將檔案放置於不同目錄。

2.有關網站之服務、格式、內容等設計如下：

(1)應符合國家發展委員會政府網站服務管理規範，並參考最新版政府網站營運績效檢核計畫檢核指標之網站介面項目優化設計。

(2)依行政院及所屬各機關行動化服務發展作業原則辦理行動化服務或行動化應用開發業務，優先開發響應式設計之網頁（RWD），次而行動化應用軟體（APP）。

(3)視需求及計畫內容，盡可能以互動性及視覺化網頁設計資料呈現方式。

(4)宜依身心障礙者權益保障法第五十二條之二規定取得國家通訊傳播委員會第一優先等級A以上之無障礙標章，一〇六年後改版或新設網站宜依第二優先等級AA標章規範進行設計。

3.設有意見信箱或討論區等使用者回饋機制者，應預防使用者大量資料輸入、企圖癱瘓系統等惡意行為；如開放檔案上傳，則應視需要限制檔案大小及格式，並正向表列可上傳之檔案格式，禁止有可執行之檔案格式。

4.網頁內容如涉本署機敏資料或個人資料者，除屬公務可公開外(如機關首長姓名、學經歷、單位主管姓名、職稱、公務電話等)，均不公開；如有需要，應於去識別化後公開。

5.為強化民眾瀏覽政府網站之安全性，應導入並預設為安全傳輸協定(HTTPS)。

七、程式開發

(一)程式撰寫原則應具一致性並結構化、命名簡單易懂、註解清楚並留存說明文件，且完整說明系統流程、各程式間關聯與資料流向。如採開源或套裝軟體改寫者，應詳加說明各模組及程式改寫內容及用途。

(二)檔案應依性質或權限，以相同原則集中於特定目錄；其中暫存檔應有容量大小限制及完善自動刪除機制、日誌檔應定期備份管理。另伺服器不應留存與專案無關之檔案。

(三)存取資料庫主機應使用 Host Name，不得使用 IP 連線；亦不得使用資料庫預設帳號登入。

(四)應配合行政院政府組態基準（GCB）政策：系統若客製化 ActiveX 元件，應提出 ActiveX 元件程式碼簽章證明、實施 ActiveX 安全性檢測（至少含弱點掃描、原始碼檢測及滲透測試等必要項目）並確保使用者環境能正常使用各系統功能及管理工具等；詳參行政院國家資通安全會報技術服務中心網站公告。

八、系統測試

(一)本階段產出之文件為測試計畫書及測試報告書(參考格式如附件四、五)。

(二)不分開發或維護階段之系統，測試工作皆限於「測試環境」中進行，測試環境並限制僅有計畫相關人員可存取。

(三)避免使用現行正式區之資料作為測試資料，如需使用現行正式區資料，應符合以下控管原則：

1.應於主辦單位同意後，由執行單位依申請內容將資料搬移至測試區。

2.針對重要敏感欄位（如身分證統一編號、住家住址、信用卡卡號等）應予以刪除或重新編碼後方可使用。

3.需於測試完畢後，立即將測試資料清除。

(四)執行單位應擬訂測試計畫書，對系統進行至少以下檢測，檢測結果應詳細紀錄於測試報告書：

1.依計畫說明書、需求規格及設計文件內容，進行系統單元測試、整合測試等各項功能測試。

2.依資通安全責任等級分級辦法附表十所規範對全系統及主機進行源碼掃描(高級需檢)、滲透測試(高級需檢)、弱點掃描(至少含 OWASP TOP 10 最新正式版)(高中普級均需檢)，及其他必要之壓力測試、GCB 符合性檢測。

(五)測試項目通過準則

1.測試個案執行結果如不符合計畫說明書、需求規格及設計文件等預期要求、或資安檢測結果存在中或高風險弱點或不符事項時，即應判為問題。

2.測試個案執行結果如有規格未明定，但依資訊系統慣例為明顯不合理或不便於使用時，亦判為問題。

3. 執行結果被判為有問題之個案，除經計畫承辦人簽奉同意列為系統限制且留有問題報告外，其測試結果即為不通過。
4. 當所有測試個案均執行完畢而未發現異常，或所有測試個案均已執行完成，即為通過測試工作。
5. 如相關人員對問題之判定有所疑義時，應報請計畫承辦人召開專案會議共同判定。

九、教育訓練

(一)計畫工作項目如訂有教育訓練，執行單位應於訓練前提交下列文件：
1. 教育訓練計畫書
2. 教育訓練簡報講義
3. 系統操作手冊

(二)教育訓練名單(或簽到表影本)如附於期末報告、會議紀錄或成果報告書時，應將個人資料(如姓名、身分證統一編號等)遮罩處理或予以刪除。

十、系統上線

(一)系統上線前應通過系統測試階段所列之各項檢測並提供證明。

(二)負責資料提供之資訊系統，需於水利資料整合雲平台註冊其資料並提供服務；其它資訊系統存取該資料前，應完成申請程序，待獲得同意後，方可進行資料存取。

(三)執行單位需撰寫系統安裝手冊(參考大綱如附件六)，詳實說明系統安裝、組態設定、排程、備份及還原等作業程序細節。

(四)新系統上線使用前應擬訂上線計畫，就主機網路環境設定、測試帳號及資料刪除、資料轉檔細節與其他系統介接切換等各項上線相關事項逐一確認，以降低系統移轉對使用者之影響。

(五)原始程式碼不得存放於系統主機上，且應存放於安全儲存空間內、保存至少近三個版次，並提供適當存取機制進行程式碼管控。

十一、系統維護

(一)系統上線運作後，應依以下規定辦理：
1. 如系統須中斷服務，應適當公告，周知使用者。
2. 功能增修等系統變更應由主辦單位視變更規模要求執行單位依本注意事項第四點至第十點之規定辦理，並一併更新各相關文件。
3. 應依資通安全責任等級分級辦法附表十資通系統防護基準之各項控制措施辦理。

(二)為瞭解執行單位資安防護現況，本署(含所屬機關)得視需要對執行單位實施資安稽核，並據以要求執行單位配合改善；涉資安疑慮未配合改善之系統，本署得中斷系統連線，或關閉系統運作至改善完成為止。

(三)系統於任一階段均應配合本署(含所屬機關)資料清查工作，視本署需要納入水資源資料交換標準管理，並應依水利資料整合雲或水資源物聯網感測基礎雲端作業平臺資料管理政策填寫文件、安裝相關程式且提供資料交換或開放。

附件

附件一　需求規格書　參考大綱

一、前言

（一)文件目的

（二)現有系統

（三)現有系統的限制、與其他系統間之關聯

二、標的應用系統摘述

（一)整體系統概述

（二)系統操作環境平台

（三)使用者作業活動

（四)驗收前應準備之文件

三、分項功能需求

（一)功能需求

（二)介面需求

（三)資安需求

（四)其他需求

四、需求驗收衡量

（一)驗收衡量項目

（二)衡量通過準則

五、軟體品質保證與稽核

六、雛型系統摘述

七、需求追溯表

八、附錄

附件二　系統需求訪談紀錄表　參考格式

(機關)系統需求訪談紀錄表

計畫名稱			
訪談主題			
時間		地點	
主持人		紀錄	
出席人員：			
訪談過程及結論			

填表說明：
如有委託服務計畫，履約前，主辦單位與需求單位訪談紀錄由承辦人填寫；履約中，機關與受託廠商雙方需求訪談紀錄由廠商填寫。

附件三　設計規格書　參考大綱

一、前言

（一）文件目的

（二）名詞解釋與縮寫符號

（三）參考文件資料

二、設計規劃

（一）設計方法與工具

（二）軟體組織架構

（三）系統流程圖

（四）軟體元件設計

（五）使用者介面設計

（六）資料結構設計

（七）資料庫設計

（八）安全性設計

（九）例外處理

三、規格追溯表

四、附錄

附件四　測試計畫書　參考大綱

一、前言

（一）文件目的

（二）名詞解釋與縮寫符號

（三）參考文件資料

二、軟體驗證計畫

（一）需求確認

（二）功能設計驗證

（三）細部設計驗證

（四）程式碼驗證

（五）安全性驗證

三、軟體確認計畫

（一）測試類別

（二）測試機制

1. 測試環境

2. 測試方法

（三）測試準則

1. 測試項目之通過失效準則

2. 測試中止及再繼續之原則

（四）測試工作時程

（五）測試應交付文件

1. 測試機制摘述

2. 測試結果彙總清單

3. 測試紀錄

4. 測試異常報告

四、附錄

附件五　測試報告書　參考大綱

一、前言

（一)文件目的

（二)名詞解釋與縮寫符號

（三)參考文件資料

二、軟體驗證報告

（一）需求確認

（二）功能設計驗證

（三）細部設計驗證

（四）程式碼驗證

（五）安全性驗證

三、軟體確認報告

（一）測試機制摘述

（二）測試結果彙總清單

（三）測試紀錄

（四）測試異常報告

（五）測試涵蓋率

附件六　系統安裝手冊　參考大綱

一、前言

二、應用系統環境需求

三、系統架構

四、安裝指南

（一)安裝步驟

（二)安裝之注意事項

五、備份程序

六、復原標準作業程序