智新資通股份有限公司

文件名稱:系統開發與維護管理程序			
文件編號:ISMS-2-015	版本:B	頁次:1/5	發行日期:2025/05/19

版本修訂紀錄表

文件版本	制/修訂日期	修訂重點內容	修訂人員
A	2023/01/07	初稿	Pake
B	2024/11/15	新增項次5.4.4安全編碼規範與5.6.3源碼掃描作業、5.6.4項次程式源碼掃描報告存放及保存規定。	Judy
C	2025/05/02	修訂增加ISO/IEC27701要求	Kasen

智新資通股份有限公司

文件名稱:系統開發與維護管理程序			
文件編號:ISMS-2-015	版本:B	頁次:2/5	發行日期:2025/05/19

1.目的

本程序書制訂之目的在於資訊系統開發、測試與維護作業之資訊安全與個人資料保護管理。

2.適用範圍

程式開發過程使用之應用系統之開發、修改、維護、上線變更、原始碼之管控與儲存等作業。

3.權責

系統開發、維護人員與委外人員:遵守本程序書之相關規定，以確保本單位相關軟體與資料等資訊資產之安全。

4.名詞定義

無。

5.作業說明

5.1 系統開發之評估

5.1.1 若有系統開發專案需求時，由業務人員取得相關業主要求或標單規格後，交開發人員進行可行性評估，如有需求時，可召開專案會議進行評估及研討。

5.1.2 於可行性評估時，需考量專案技術需求、資源充裕性及資訊安全、個人資料保護需求。

5.1.3 評估結果需記錄於「專案評估表」，評估其可行性及預估工時。

5.1.4 評估結果交PM進行確認，並產出相關服務建議文件，並將評估結果詳細描述。

5.2 需求訪談

5.2.1 立案後，由PM及開發人員與業主進行需求訪談，以確認細部規格要求。

5.3 專案規格確認後，由PM立案管理，並產出製作工作計畫文件或期初報告，列管相關工作項目、項目起迄時間及負責人。

5.4 系統設計及分析

5.4.1 由開發人員進行系統設計及分析作業，並由PM彙整結果於系統分析及設計報告文件。

5.4.2 於系統設計及分析時，需考量系統開發安全需求，由開發單位主管依「系統安全需求項目查檢表」進行安全需求分析，已確認系統安全規格。

5.4.3 應用系統個人資料安全規則

智新資通股份有限公司

文件名稱:系統開發與維護管理程序			
文件編號:ISMS-2-015	版本:B	頁次:3/5	發行日期:2025/05/19

5.4.3.1 確認蒐集之個資，是否符合最小化原則。

5.4.3.2 如以應用系統進行當事人個資蒐集及處理同意選擇時，選項不宜預設同意。

5.4.3.3 於應用系統發展時，以最小化原則進行個資揭露、存取及保存。

5.4.3.4 程式設計應對個資的輸入加以過濾，並檢核資料之適當性。

5.4.3.5 針對個資欄位的輸入，如為已知之資料範圍，宜提供選單或選項之方式進行輸入。

5.4.3.6 進行個資強制輸入檢查，並限制前端應用程式資料輸入的長度與型別，另於輸入個資時使用適當之顯示隱碼功能。

5.4.3.7 應用系統於個資作業產出暫存檔，宜規劃刪除之機制。

5.4.3.8 應用系統個資檔案應規劃最小化之保留期間要求。

5.4.3.9 個資檔案於保留期限後進行刪除作業，並以無法回復之方式進行刪除作業。

5.4.3.10 個資檔案進行傳輸時，宜考量安全機制(如加密傳輸、存取控制)。

5.4.4 應用系統稽核日誌安全規則請參照「稽核日誌安全作業規範」。

5.4.5 如業主有系統開發安全要求時，及依業主要求執行。

5.4.6 於專案開發作業時，需依客戶要求進行編碼，如客戶無特殊要求時，則參照「應用系統安全編碼作業規範」進行編碼，以確保開發結果符合安全要求。

5.5 測試及驗收

5.5.1 由開發人員依系統規格產出測試計畫文件，並於開發完成後，需依測試計畫文件進行測試。

5.5.2 測試人員測試完成後，產出測試報告文件，以確保開發結果符合規格要求。

5.5.3 系統開發安全需求之確認，由PM依「系統安全需求項目查檢表」之評估結果進行確認，並紀錄於「系統安全需求項目查檢表」。

5.5.4 系統開發測試資料涉及機密性時，需以虛擬資料進行測試，不可使用真實資料進行測試。

5.5.5 系統增修作業完成後，程式設計人員須進行測試，測試作業須於測試電腦上執行，或於獨立虛擬環境，不可於正式環境中進行測試。

5.5.6 系統驗收作業依照業主要求或標單規格執行，並留下驗收相關紀錄備查。

5.6 系統安全管理

智新資通股份有限公司

文件名稱:系統開發與維護管理程序			
文件編號:ISMS-2-015	版本:B	頁次:4/5	發行日期:2025/05/19

5.6.1 其他系統安全測試(如弱點掃描、原碼掃描),依業主要求執行,並留下相關測試及修訂之報告。

5.6.2 如業主無特定要求時,由開發單位進行弱點掃描,並針對中、高風險項目進行回覆,並產出「弱點掃描回應報告」。

5.6.3 專案交付前,進行源碼掃描,針對中/高風險項目進行回應,並進行複掃,以確認編碼之安全性。

5.6.4 針對程式源碼掃描報告,須由系統部門存放於指定資料夾,並針對其存取加以限制,僅允許系統部門存取,並針對同一專案,至少保留最後三次源碼掃描紀錄。

5.6.5 於公共網路上提供服務之應用系統,宜考量其業主要求、資訊機密性及風險程度,建立適當之加密機制,以防止詐欺活動、契約爭議及未經授權揭露與修改,並保護應用服務交易。

5.6.6 本公司軟體開發作業使用之套裝軟體不作變更作業。

5.7 版本控管

5.7.1 系統正式上線後,系統維護所需之相關軟體及文件應進行版本控管。

5.7.2 對於保存相關軟體及文件電子檔之環境,應進行權限控管與防毒等管制,以防止資料被盜用、誤用、未授權之無意或惡意竄改、受病毒破壞等事件發生,對資料亦應進行備份。對於紙本形式之相關維護文件,亦應進行存取及防護之管制。

5.7.3 系統需進行軟體或文件變更時,變更內容應加以述明,欲變更項目應先確認並備份,以利必要時進行復原。

5.7.4 對於已變更之項目,應先行由修改人員進行適當之驗證與測試,變更項目驗證與測試無誤後,經權責人員核准後,始得進行變更項目之更替。

5.7.5 對於因緊急維護狀況須變更之系統,應於事後將相關資料補齊,以利追蹤與查核。如系統維護作業是根據需求人員問題提報而執行,於維護完成後,由系統維護人員將結果回報給原問題提出人員。

5.7.6 原始碼應加以保存,並按其版次狀況予以識別管理,並針對原始碼之存取設定權限管理。

5.8 為防止資訊系統開發或設備採購過程中,因為軟體技術的瑕疵,造成系統隱患的風險,依需求,應在系統開發技術或驗收文件中載明可能有的系統弱點資訊,並且評估該弱點暴露的程度及所造成的可能風險。

6. 相關文件:

6.1 應用系統安全編碼作業規範(ISMS-3-002)

6.2 稽核日誌安全作業規範(PIMS-3-001)

7. 使用表單:

7.1專案評估表(ISMS-2-015-01)

7.2系統安全需求項目查檢表(ISMS-2-015-02)

7.3弱點掃描回應報告(ISMS-2-013-02)