管理系統文件

文件類別	第二階文件	
文件編號	ISMS-P-014	
文件名稱	系統發展與維護管理程序書	
發行單位	文件管制小組	
發行日期	111 年 02 月 17 日	
版次	2.3	
訂修廢單位	審查	核准
資通安全處理小組		

（原版簽名頁保存於資通安全處理小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
2.0	104/04/30	2015 改版發行。
2.1	107/03/09	修改本文件 5.1.及 5.2.1.1.1.權責單位資訊科技中心單位名稱為圖書資訊處。
2.2	108/04/15	因應資通安全管理法修訂本文件。
2.3	111/02/17	新增 5.10.10 容量管理程序。 新增 5.10.9.4.4 重要系統稽核日誌（Log）之留存期限程序。

1. 目的

為促使本校委外或自行開發之資通系統在取得、發展與維護有一明確之規範，以確保應用系統之安全性，特制訂本程序書。

2. 適用範圍

凡本校委外或自行開發應用系統之取得、發展與維護管理，均適用本程序書。

3. 參考文件

3.1. ISMS-P-018 委外作業管理程序書。

3.2. ISMS-P-013 帳號密碼及存取控制管理程序書。

3.3. ISMS-P-009 資通安全事件通報及應變管理程序書。

3.4. ISMS-P-015 資訊備份管理程序書。

3.5. ISMS-P-008 矯正及預防管理程序書。

4. 名詞定義

4.1. 應用系統

泛指套裝軟體以外且由本校自行開發或委由外部廠商開發之各項應用管理系統稱之。

5. 作業內容

5.1. 系統發展與維護管理流程圖

作業流程	權責單位	相關表單
確立系統開發需求	需求單位	校務資通系統需求反應單（線上表單）
No / 評估及審查	需求單位/圖書資訊處	
Yes / 系統分析	圖書資訊處/廠商	
No / 規格確認	需求單位	
Yes / 系統開發建置	圖書資訊處/廠商	
No / 系統測試	需求單位/圖書資訊處	
Yes / 輔導系統上線	圖書資訊處/廠商	系統說明文件/系統操作手冊
No / 技術轉移或編寫技術文件	圖書資訊處/需求單位	
驗收	圖書資訊處/廠商	
Yes / 系統維護與管理		
紀錄保存		

5.2. 系統發展安全政策與原則

5.2.1. 組織的系統發展安全政策應從開發環境安全、軟體開發生命週期中開發方法論及安全程式碼（Secure Code）、設計階段安全要求、安全儲存、版本控制及開發人員具防止、發現和修復安全漏洞的能力。

5.2.2. 系統發展工程安全程序應基於安全工程原則建立，並應運用於本公司內部資通系統開發活動，安全的設計應考量系統架構，以平衡資通安全與存取需求；並應對新技術進行安全風險分析，且對已知的攻擊模式與漏洞定期檢視，以確保系統發展過程符合安全要求。

5.2.3. 相關安全工程原則亦適用資通系統委外開發，並應納入合約規範並定期檢視，以確認供應商系統開發遵從相關安全程序與原則。

5.3. 確立系統開發需求與評估審核

5.3.1. 應用系統需求申請

5.3.1.1. 系統自行開發

5.3.1.1.1. 本校各單位依業務實際需求，上網於報修系統填寫「校務資通系統需求反應單」(線上表單)，並經單位主管核准後，向圖書資訊處提出應用系統需求之申請。

5.3.1.1.2. 由承辦人員負責規劃與設計需求單位之應用系統。

5.3.1.2. 系統委外開發

5.3.1.2.1. 本校所需之應用系統經評估其可行性後，提請相關需求單位辦理系統委外開發提案與編列預算。

5.3.1.2.2. 審核通過列入年度預算之應用系統委外開發案，得依本校採購程序及本程序書之應用系統安全要求，進行委外採購。

5.3.1.2.3. 由承辦人員協助審查應用系統之資通技術與提供支援。

5.3.2. 系統委外發展專案規劃

委外專案應協助需求單位，由需求單位依據本校相關採購流程，

進行委外採購程序，並注意以下事項：

5.3.2.1. 任何性質之專案需求，必須在「需求規格書」中清楚明確的定義與表達。

5.3.2.2. 專案委外採購時，簽約廠商應進行專案細部規劃，並提出「專案執行計畫書」，內容必須包含發展時程、效益與人力需求分析與應用系統所應達成的功能。

5.3.2.3. 本校委外作業，應依據「ISMS-P-018 委外作業管理程序書」之規定辦理。

5.4. 系統分析

5.4.1. 一般要求

5.4.1.1. 進行系統需求單位之資訊收集，包含下列資料：

5.4.1.1.1. 需求單位現行各項作業表單（含報表）。

5.4.1.1.2. 需求單位內部之相關管理文件。

5.4.1.2. 系統採委外開發時，系統開發廠商需要會同承辦人員，對於需求單位進行需求訪談。

5.4.1.3. 自行發展之應用系統，由需求單位使用者進行需求訪談。

5.4.1.4. 系統開發廠商依據資料收集及訪談結果，撰寫系統開發相關文件。

5.5. 規格確認

5.5.1. 系統開發應依據系統開發相關文件與需求單位進行規格確認，包

含下列事項：

5.5.1.1. 確認應用系統作業流程。

5.5.1.2. 確認使用者操作畫面。

5.5.1.3. 確認系統可產出的管理報表格式。

5.5.1.4. 確認資料庫資料格式與欄位。

5.6. 系統開發建置

5.6.1. 依據系統分析及規格確認結果進行系統程式開發。

5.6.2. 應用系統安全規範
應用系統進行開發時須包含以下安全要求：

5.6.2.1. 身分驗證

5.6.2.1.1. 系統應具備檢驗登入身分識別與密碼功能。

5.6.2.1.2. 無法使用作業系統提供的驗證機制，則需在應用系統中使用自訂驗證機制。

5.6.2.1.3. 使用者登入應用系統後，若超過所規定的閒置時間而無任何動作時，系統須設定將其帳號登出（若屬功能限制或系統老舊無法提供此功能，待版本升級或更新系統時改善）。

5.6.2.2. 權限管理

5.6.2.2.1. 應用系統權限應視使用者業務需求，給予不同角色並對應適當權限。

5.6.2.2.2. 應用系統應紀錄使用者處理敏感性資訊交易之相關資訊。

5.6.2.3. 系統錯誤處理

5.6.2.3.1. 應用系統應該實作且具有例外狀況處理機制，以擷取錯誤資訊。

5.6.2.3.2. 例外狀況管理包含擷取和回傳例外狀況、設計例外狀

況、傳送例外狀況資訊，並避免直接顯示原始完整錯誤資訊給予使用者。

5.6.2.4. 資料庫存取安全

5.6.2.4.1. 資料庫連接字串之產生，應對於字串的輸入加以過濾，並限制長度，例如單、雙引號都應過濾。

5.6.2.4.2. 加強資料庫帳號與權限管理，應用程式連結帳號權限應考量賦予最小之必要權限，系統管理者的帳號應視需要予以管制使用。

5.6.2.5. 系統輸入檢查

5.6.2.5.1. 針對資料欄位的輸入，如為已知之資料範圍，應提供選單或選項之方式進行輸入。

5.6.2.5.2. 應用系統應具備資料輸入及輸出錯誤之檢查機制，並提示使用者輔助資訊，確保資訊輸入輸出的正確與完整。

5.6.2.5.3. 進行資料強制輸入檢查，並且限制前端應用系統資料輸入的長度與型別，並於輸入敏感資訊時使用適當之顯示遮罩功能。

5.7. 系統測試與輔導系統上線

5.7.1. 系統測試

為確保應用系統符合本校需求單位之需求，須依以下之規範進行相關系統測試。

5.7.1.1. 進行測試前，應建構測試環境及測試案例，同時分析並調整測試案例，以提高測試效率。

5.7.1.2. 系統如透過網路存取，應執行適當之防駭測試。

5.7.1.3. 測試資料由需求單位提供或以模擬資料進行，禁止使用具有安全考量之測試資料。

5.7.1.4. 測試系統與正式系統所使用之環境、資料應獨立分開。

5.7.1.5. 系統測試需經開發者與使用者至少各一人以上進行測試。

5.7.1.6. 測試資料除了進行正常資料測試外，並需測試不正常之資料輸入，如過長或過短的輸入資料、輸入格式錯誤的資料、可能造成緩衝區溢載之大量輸入資料等，以及早發現系統問題。

5.7.2. 輔導系統上線

5.7.2.1. 上線前應進行系統備份，並通告相關人員系統上線期間之影響。

5.7.2.2. 上線過程若遇問題無法排除，應立即進行回復作業，並進行原因分析與重新評估上線程序。

5.8. 技術轉移或編寫技術文件

5.8.1. 技術轉移

適用於資通系統委外發展之專案。

5.8.1.1. 由委外廠商到本校舉辦系統軟體技術轉移說明會，技術轉移內容必須包含下列事項：

5.8.1.1.1. 作業系統、資料庫及系統程式安裝。

5.8.1.1.2. 系統及網路相關參數設定。

5.8.1.1.3. 開發工具安裝。

5.8.1.1.4. 系統安全設定。

5.8.1.1.5. 網路環境設定。

5.8.1.1.6. 辦理系統操作及使用訓練。

5.8.1.2. 委外廠商應提交下列相關資料：

5.8.1.2.1. 系統操作及使用手冊文件。

5.8.1.2.2. 資料庫檔案結構說明。

5.8.1.2.3. 原廠的系統使用授權書。

5.8.2. 編寫技術文件

適用於資通系統自行發展之專案。

5.8.2.1. 由系統開發人員編寫「系統說明文件」做為日後維護與管理使用。

5.8.2.2. 由本校編寫「系統操作手冊」提供使用者參考使用。

5.9. 驗收

5.9.1. 系統委外採購時，依本校驗收流程會同權責單位及需求單位辦理驗收作業，並將驗收結果呈送權責主管審核備查。

5.9.2. 經驗收不合格的項目，廠商須限期改正，並另擇日驗收以符合契約之驗收規定。

5.10. 系統維護與安全管理

5.10.1. 系統帳號及權限管理

5.10.1.1. 應用系統之管理帳號與使用者帳號、密碼與權限管理原則，須依據「ISMS-P-013 帳號密碼及存取控制管理程序書」之規定，妥善保存及管理系統帳號及密碼。

5.10.1.2. 系統使用權限指派考量，應僅賦予應用系統使用者適當的權限，以降低誤用系統的風險。

5.10.1.3. 因個人基本資料保密考量，各應用系統應建立防止未授權使用列印之功能。

5.10.1.4. 人員停職、離職或調職時，應依據本校離調職作業流程通知帳號管理者，進行人員帳號停用、刪除或變更。

5.10.1.5. 應用系統使用者存取行為，系統應保存適當紀錄，以便後續追蹤與蒐證，提供相關單位進行查核。

5.10.2. 系統使用需求

5.10.2.1. 若需應用系統之使用權限，使用者應須依據「ISMS-P-013 帳號密碼及存取控制管理程序書」規定填寫系統使用權限申請單，說明欲申請之系統名稱、帳號種類及相關細節，經權責主管核准後，向應用系統管理者提出申請。

5.10.2.2. 委外廠商或外單位人員如需使用管理者帳號進行應用系統

之維護與管理時，應經單位主管核准後始可進行，並且系統管理者於委外廠商或外單位人員作業完成後立即停用該帳號。

5.10.2.3. 使用單位因業務需求，需新增或修改應用系統時，應經單位權責主管核准後，向系統管理者提出申請。

5.10.3. 系統帳號設置

5.10.3.1. 應用系統之帳號、密碼及使用權限之建立與管理，應依據「ISMS-P-013 帳號密碼及存取控制管理程序書」之相關規定，進行系統使用帳號之設置。

5.10.3.2. 應用系統帳號建立、授權及相關設定作業完成後，使用者於初次使用時應立即變更預設密碼（若屬功能限制或系統老舊無法提供此功能，待版本升級或更新系統時改善）。

5.10.4. 系統使用測試

5.10.4.1. 使用者經單位主管核准後，取得系統使用授權，由應用系統管理者協助進行系統之使用。

5.10.4.2. 系統安裝完成後，系統管理者會依使用者所申請之帳號及密碼，進行首次系統登錄，進行系統測試以確認系統正常運作，並由系統管理者詳細告知使用者系統使用之安全規範。

5.10.5. 系統使用

5.10.5.1. 使用者於使用應用系統時，若發生系統使用之問題，應立即通知系統管理者進行問題處理，若屬資安事件時，應依據「ISMS-P-009 資通安全事件通報及應變管理程序書」之規定進行處理。

5.10.5.2. 應用系統在用戶端、伺服器與網路應用程式方面，如有授權限制，應符合授權契約條款使用軟體。

5.10.6. 應用系統變更

5.10.6.1. 應用系統若需進行變更時（如：新增功能或改善需求...等），須上網於報修系統填寫「校務資通系統需求反應單」，經主管核准後通知系統開發人員或委外廠商進行處理，並告知需求

單位處理結果。

5.10.6.2. 變更之設定項目需詳加記錄，如網路、作業系統設定或參數調整，以供後續管理上參考。

5.10.6.3. 應用系統變更如以遠端連線方式進行，則須依「ISMS-P-018 委外作業管理程序書」之規範開啟網路存取權限，在系統管理者之監控下進行系統變更。

5.10.6.4. 應用系統變更前，應評估對各使用單位之影響並通告各相關單位協調系統變更時間，以降低對業務運作之影響。

5.10.6.5. 應用系統完成變更作業後，應更新相關系統文件。

5.10.7. 應用系統維護

5.10.7.1. 應用系統有資料庫異動需求時，需求單位須上網於報修系統填寫「校務資通系統需求反應單」，經權責主管核准後方可對資料庫進行異動作業。

5.10.7.2. 每月由應用系統管理者，針對應用系統維運與軟硬體進行檢查；若系統為委外處理，則須要求委外廠商定期實施系統檢查，並將檢查結果回覆給系統管理者，以確保系統之維運與安全。若發生異常事件，則由系統管理者進行異常處理。

5.10.7.3. 檢查紀錄時需檢視是否符合應用系統服務品質目標之設定，以供單位主管不定期檢視系統運作狀況，作為維護、擴充系統及日後改善之參考。

5.10.7.4. 應用系統使用者發現系統有異常情形，應立即通知報修。

5.10.7.5. 本校與委外廠商所簽訂之相關維護合約內容，依據合約內規範通知廠商處理。

5.10.8. 應用系統之安全管理

5.10.8.1. 應用系統於規劃建置時之初，即應評估所處理資料之重要性，並依據評估結果，採購適當之系統軟、硬體或利用適當的資料儲存技術（如：磁碟陣列、儲域網路技術）進行資料的存放，以滿足資通安全之需求。

5.10.8.2. 儲存空間之規劃並應考慮未來資料量的成長趨勢，避免發生資料儲存空間不足的情況。

5.10.8.3. 對於上線之各應用系統，除主要資料儲存空間之規劃考量外，平時亦須進行適當之資料備份，備份作業應依據「ISMS-P-015 資訊備份管理程序書」之規定辦理。

5.10.8.4. 應用系統管理者或使用者，對於使用或控管流程須負有保密之責。

5.10.8.5. 處理機密資料之應用系統，若採取委外開發，應謹慎考慮業務機密洩漏之風險，並遵守「ISMS-P-018 委外作業管理程序書」之規範。

5.10.8.6. 應用系統如有程式安裝光碟或是程式原始碼光碟，應由應用系統保管人負責保管。

5.10.8.7. 應用系統開發過程中，如有使用商業軟體元件（如：COM、API 等），應取得合法使用授權後始得使用，並注意該商業軟體元件授權相關規定。

5.10.9. 資料庫之安全管理

5.10.9.1. 資料庫安全存取控制

5.10.9.1.1. 使用資料庫須經資料庫管理者進行身分認證與權限管理，且須使用獨立之帳號及密碼登入。

5.10.9.1.2. 進行資料庫存取之身分驗證機制，須由系統內部安全機制提供。

5.10.9.1.3. 系統管理者須建立專屬帳號，不得多人共用同一帳號。

5.10.9.1.4. 資料庫使用者之帳號密碼設定必須依據「ISMS-P-013 帳號密碼及存取控制管理程序書」之相關規定辦理。

5.10.9.1.5. 資料庫公用程式路徑之存取權限應適當控管，禁止一般使用者存取。

5.10.9.1.6. 資料庫最高權限帳號之存取授權應僅限於資料庫管理者。

5.10.9.1.7. 資料庫預設帳號應變更密碼，或是關閉使用。

5.10.9.1.8. 僅系統管理者擁有異動資料庫相關檔案的作業權限。

5.10.9.1.9. 除系統管理者外，非經授權禁止直接連接資料庫進行新增、修改與刪除等作業。

5.10.9.2. 資料庫管理系統安全性

5.10.9.2.1. 針對資料庫系統已知漏洞，在不影響現行作業狀況下，應立即進行修補。

5.10.9.2.2. 應用程式禁止使用資料庫管理者帳號連結資料庫進行存取。

5.10.9.2.3. 為確保資料庫內資料之安全性，針對資料庫之權限控管制定原則，資料庫存取帳號、權限應視不同應用系統、人員存取之需求進行適當設定。

5.10.9.3. 資料庫備份

5.10.9.3.1. 重要資料庫應定期備份，並且抽檢備份資料是否可用。

5.10.9.3.2. 資料庫備份之存放點應進行控管，防止非相關人員存取。

5.10.9.3.3. 資料庫備份請依據「ISMS-P-015 資訊備份管理程序書」之規定辦理。

5.10.9.4. 資料庫存取稽核紀錄

5.10.9.4.1. 資料庫系統在不影響正常運作之效能，針對存放敏感性資料啟動相關安全稽核紀錄功能（包含異動）。

5.10.9.4.2. 僅授權之人員可讀取資料庫稽核紀錄。

5.10.9.4.3. 系統管理者應不定期檢視資料庫稽核紀錄，防止資料庫不當操作與存取。

5.10.9.4.4. 重要系統稽核日誌（Log）之留存期限，應依據「ISMS-P-11 實體與環境安全管理程序書」要求作業，以確保資料完整性及有效性。

5.10.10. 容量管理

5.10.10.1. 資源的使用應予監控、調整和預測，並考量未來的容量需求，以確保所需的系統性能。

5.10.10.2. 容量需求應被識別，並優先考量核心系統及關鍵營運流程；重要系統應調校，並依據「ISMS-P-11 實體與環境安全管理程序書」有關「ISMS-P-011-03 管制區域檢查表」進行監控，以確保可增進系統可用性與效率。

5.10.10.3. 未來的容量需求預測應考慮新的業務和系統需求，以及組織資通處理能力的當前狀態與未來趨勢。

5.10.10.4. 管理者應該利用相關資訊來識別和避免潛在的瓶頸，以及可能對系統的安全性或服務產生威脅的人員，並採取適當行動。

5.10.10.5. 適切管理容量可參考作法，包括（但不限於）：

5.10.10.5.1. 刪除過時的數據（磁碟空間）。

5.10.10.5.2. 關閉應用程式、系統、資料庫或操作環境。

5.10.10.5.3. 優化批次處理和排程。

5.10.10.5.4. 優化應用邏輯或資料庫查詢。

5.11. 異常處理

5.11.1. 發生資安事件時，應立即依據「ISMS-P-009 資通安全事件通報及應變管理程序書」所訂定之通報管道，迅速通報單位主管及系統管理者進行問題處理。

5.11.2. 異常狀況無法有效解決時，應依據「ISMS-P-008 矯正及預防管理程序書」之相關規定執行矯正與預防措施，進行問題矯正及風險預防的作業，確保問題不再發生。

6. 附件

無。