

國立空中大學系統開發與維護程序書

經 98 學年度第 2 次資訊環境規劃委員會通過 (99.6.1)

經 99 學年度第 1 次資訊環境規劃委員會修訂通過 (99.12.28)

1. 目的

國立空中大學（以下簡稱本校）為開發、測試與維護資訊系統（含網頁製作）特訂定本程序書。

2 適用範圍

本校施作範圍內資訊系統（含網頁製作，以下提及系統均含網頁製作）之程式開發相關支援活動，如既有線上系統之測試、修改、維護、上線變更、原始碼之管控與儲存等作業。

3 權責

本校相關資訊系統（含網頁製作）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 一般控制措施

- 5.1.1 當發展新資訊系統，或現有系統功能之強化，於系統規劃需求分析階段，即將安全需求要項納入系統功能。
- 5.1.2 除由系統自動執行之安全控管措施之外，亦可考量由人工執行相關控管措施。
- 5.1.3 於採購套裝軟體時，視其安全需求，進行分析。除事前經軟體使用單位主管核准外，應避免修改套裝軟體，如需修改應依本程序書之變更作業控制措施加以控管。
- 5.1.4 系統之安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足，可能帶來之傷害程度。
- 5.1.5 資訊系統應保護敏感等級（含）以上之資料，防止洩漏或被竄改，必要時應使用資料加密等技術保護。
- 5.1.6 在作業系統上執行應用軟體，應建立控制程序並嚴格執行，為減少可能危害作業系統之風險，應用程式之更新作業應限定只能由授權之管理人員才可執行，且應建立應用程式之更新稽核紀錄。
- 5.1.7 真實資料被複製到測試系統時，應依複製作業之性質及內容，在取得授權後始能

進行且需對真實資料進行適當遮蔽掩蔽。真實資料之複製情形應予以紀錄，以備日後稽核之用。

5.1.8 系統若需委外建置或維護，請參考「國立空中大學資訊委外服務資訊安全管理事項」。

5.1.9 系統弱點管理，應定期查核技術符合性，進行弱點掃描或滲透測試，以確定資訊系統及網路環境符合安全實施標準。掃描週期如下：

5.1.9.1 每半年至少針對伺服器執行一次。

5.1.9.2 當系統有重大變動時。

5.1.9.3 新系統上線前。

5.1.10 資訊如涉及重要資料之傳輸，應使用加密傳輸，並依下列規定進行金鑰之管理：

5.1.10.1 金鑰應有明確的啟動與止動日期，並於可用期間，保護其不被修改、遺失和破壞。

5.1.10.2 系統端金鑰之使用與存取，應限於金鑰之系統管理者，不可由其他非系統管理者任意存取。

5.1.10.3 使用者端金鑰之使用，應限於權責單位承辦人員，用畢應鎖於安全之處所或專人保管。

5.1.10.4 對於金鑰之使用、啟動、止動，皆應留存相關之稽核紀錄。

5.2 軟體控制措施

5.2.1 作業系統變更時，應審查與測試重要營運系統，以確保對組織作業或安全無不利之衝擊。

5.2.2 系統軟體安裝：系統軟體應由系統負責人進行安裝，安裝時應視狀況通知相關技術人員支援或通知使用者，以避免資訊服務中斷或影響業務。

5.2.3 系統軟體測試

5.2.3.1 軟體測試由系統負責人辦理，測試時應事先公告並通知協調相關人員支援。

5.2.3.2 系統負責人應通知相關人員及使用者以避免資訊服務中斷或影響業務。

5.2.3.3 系統軟體更新：系統負責人需定期檢視更新系統安全修補、防毒軟體及防毒碼，以維持系統正常運作。

5.3 開發作業控制措施

5.3.1 提案與回覆

- 5.3.1.1 申請單位提出「系統需求申請與回覆單」敘明需求理由。
- 5.3.1.2 承辦人員於完成與申請單位之訪談與系統分析後，於「系統需求申請與回覆單」中回覆評估結果，包含功能細項、預估人力與時程、建議方案等。
- 5.3.2 分析規劃與程式撰寫
 - 5.3.2.1 程式開發者應於程式開發前進行系統分析，系統分析時應將系統安全需求納入考量。
 - 5.3.2.2 輸入應用系統之資料，應檢查主要欄位或資料檔案的內容，以確保資料的有效性與真確性。
 - 5.3.2.3 對高敏感性的輸入資料，必要時應採用資料保密機制，在傳輸或儲存過程中應採加密方法保護。
 - 5.3.2.4 輸出之資料，應於輸出之前，確認其正確性；對於系統內之訊息，則需保護其完整性。
- 5.3.3 測試
 - 5.3.3.1 測試環境與線上環境應予以分開。
 - 5.3.3.2 程式設計初步完成後，準備「系統測試總表」通知申請單位進行聯合測試，並請申請單位於「系統測試總表」中填寫測試結果，測試完成後填寫「系統測試報告」。
 - 5.3.3.3 程式功能若無法達成申請單位預定需求，則請系統開發人員另行修改程式後，擇期再測試，直至符合預定需求為止。
- 5.3.4 上線與驗收
 - 5.3.4.1 聯合測試進行順利完成後，進行相關驗收作業，並請申請單位簽收「系統功能驗收表」。
 - 5.3.4.2 若原系統已經存在，應於系統上線前訂定「系統上線及緊急復原計畫表」，內容包含系統轉換規劃，轉換備援處理等。
 - 5.3.4.3 系統上線後，程式開發者應提出系統功能說明文件，內容可包含「系統分析設計書」、「系統作業流程圖」、「系統資料庫說明表」，以及「系統程式碼清冊」、「使用者操作手冊」、「系統管理手冊」，及依需求提供原始程式碼等。
 - 5.3.4.4 系統若委由其他單位開發時，應請開發單位交付系統功能說明文件，由

本單位程式開發權責單位審閱，並留存備查。

5.3.5 後續系統增修維護

5.3.5.1 專案上線後功能如需修補，申請單位應填「資訊系統需求反應單」，程式開發權責單位依需求規格進行訪談規劃設計。

5.3.5.2 程式開發權責單位完成系統增修作業後與申請單位進行測試驗收結案。

5.4 變更作業控制措施

5.4.1 變更作業應考量之事項：

5.4.1.1 在實際執行變更作業前，變更作業之細項建議，應取得權責主管人員之核准。

5.4.1.2 應確保系統變更作業不致影響或破壞系統原有的安全控制。

5.4.1.3 系統開發或變更，應更新系統文件。

5.4.1.4 程式維護時，應在程式內以註解說明異動部分。

5.4.1.5 所有系統變更作業請求，皆應建立紀錄供稽核運用。

5.4.2 變更作業之控制流程：

5.4.2.1 在實際執行變更作業前，申請者應先填具「系統需求申請與回覆單」提出變更需求，並經權責主管人員核准確認。

5.4.2.2 變更作業如有需要，應會辦相關人員配合。

5.4.2.3 上線前應先進行測試，必要時請相關人員配合建置測試環境。

5.4.2.4 除非事先經由權責主管人員核准外，測試不應在線上營運系統執行。

5.4.2.5 測試完成後，申請者應擬定「系統上線及緊急復原計畫表」，決定上線日期，經權責主管人員確認後始得上線。

5.4.2.6 上線後應立即於線上營運系統再行測試，以確認系統運作正常。測試人員不得與程式開發者為同一人，以減少錯誤機會發生。

5.4.2.7 上線後測試如發現狀況，應嘗試可否立即排除，如無法立即排除，應依「系統上線及緊急復原計畫表」，回復上線前原狀。

5.4.2.8 變更作業完成後應修改相關系統設計與功能規格書。

5.4.2.9 如遇突發狀況，應經系統管理單位主管授權後，進行緊急應變處置。