法務部

資訊應用系統開發維護安全管理規範

安全分級：■ 公開 □ 一般 □ 限閱

文件編號：21401

版次：1.2

施行日期：中華民國 103 年 10 月 25 日

版本修訂紀錄表

文件版本	修訂日期	修訂內容	修訂單位	修訂人	文件管制員
1.0	96.3.13	為確保本部系統安全與正常運作，特訂定本管理規範以為依循。	資訊處	郭俊祥	郭俊祥
1.1	97.3.3	為配合矯正機關自營產品展售商城，確保網站資料傳輸及交易過程之安全性，增第八點電子商務網站安全管理條文，以規範電子商務相關事宜。	資訊處	郭俊祥	郭俊祥
1.2	103.9.10	為強化本部資訊應用系統開發安全性，增加符合安全系統開發生命週期(SSDLC)規範	資訊處	陳明照	李國鋒

目錄

一、目的

為確保法務部（以下簡稱本部）系統安全與正常運作，特訂定本管理規範以為依循。

二、適用範圍

本部資訊處自行開發、委外、購置之應用系統。

三、系統開發生命週期（SDLC）管理

（一）需求分析階段

應用系統新增或變更需求分析，除應考量可行性及成本效益外，亦應考量對現有環境之影響。

（二）規劃階段

１、應用系統規劃及既有應用系統改版時，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），來達成應用系統之安全要求。

２、委外開發之應用系統開發或變更時，應視應用系統之複雜程度與重要性，考慮要求廠商提出或修正下列文件後，始得變更：

（１）系統功能架構圖。

（２）系統流程圖。

（３）系統環境需求說明文件。

（４）需求變更明細表。

（５）會談紀錄。

３、規劃階段應確保系統安全品質，包含應用系統對於網路環境、運作環境及內外部資源使用之安全性。

（三）開發、變更與測試階段

１、系統測試與開發環境，應與正式應用系統實體區隔。

２、委外開發測試資料，如內容涉及敏感或有價性資料原則不交付廠商；如業務需求須交付者應考量採用亂碼化處理。

３、系統開發應注意智慧財產權及著作權等問題，委外開發時應註明智慧財產權及著作權之歸屬，避免出現違法情形。

４、程式撰寫時應考量安全問題，避免出現已知之弱點。

５、系統開發完成後應進行測試，除測試系統功能外，亦應測試系統安全性，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，應將該程式退回，

並請廠商或開發人員提出相關說明並修正程式。

6、開發完成之應用系統或程式經測試後，應確認符合本程序相關要求俾利作為驗收依據。

7、系統進行較大變更時，應申請經授權後始進行變更，變更範圍須經測試後始得上線運作。

（四）上線階段

1、系統相關文件，如使用者手冊、系統說明文件等，應於系統上線前提出。

2、應用系統配合上線應辦理相關教育訓練。

3、上線使用之應用系統時，應符合以下最低要求：

（1）應用系統之密碼機制強度應符合本部相關規範。

（2）應能明確建立權限劃分設定。

（3）應能提供系統存取、帳號密碼變更之系統紀錄功能。

（五）前述各階段均應同步以安全系統開發生命週期（SSDLC）檢核表進行安全檢核。

四、確保系統之正確處理

應用系統之設計應能符合對於資料輸入輸出之確認、系統內部處理及系統與系統間資料銜接之完整性，並確保系統紀錄訊息之完整性。

五、系統存取控制之管理

（一）應用系統應能管控經授權使用者可輸入及存取之資料範圍，以避免輸入及輸出錯誤。

（二）應用系統存取其他作業系統或資料庫所使用之帳號，應避免寫入程式中，並應考量應用系統所需使用之權限，應盡量避免直接使用系統最高權限。

（三）應用系統使用者帳號及密碼管理應依本部相關規範辦理。

六、檔案及資料之保護

（一）作業系統變更（版本升級、軟體安裝或設定變更等），應再評估對應用系統之影響。

（二）若需使用敏感性測試資料，測試環境之安全管控應比照正式營運環境，對於所使用之測試資料應加以保護。

（三）為確保重要系統之資料安全，資料傳輸、儲存等採用加密方式

為原則。

（四）應用系統程式碼應指定專人管理，發展中或是測試中的應用程式，應與營運之系統程式碼區隔。

（五）系統文書及相關作業手冊等資料，應依文件相關規定妥善保存。

七、系統操作與維護管理

（一）應用系統應定期審查系統或資料存取狀況，並檢驗是否有資訊被揭露之弱點存在。

（二）應建立應用系統技術脆弱性資訊之取得管道，並應評估相關可能帶來之風險。

八、電子商務網站安全管理

（一）應以 SSL（Secure Socket Layer，安全插槽層）等加密機制，確保網站傳輸消費者個人資料之機密性。

（二）應確保網站資訊之正確性，確保交易過程之安全性及防治網路詐欺行為發生（如：商品價格資訊、出貨資訊等）。

（三）應確保交易訂單、付款資訊、運送地址資訊及出貨通知之機密性及完整性。

（四）應進行買賣雙方確認作業，避免付款及出貨過程之糾紛。