

法務部資訊應用系統開發維護安全管理規範

第三點修正對照表

修正規定	現行規定	說 明
<p>三、系統開發生命週期 (SDLC) 管理</p> <p>(一)需求分析階段</p> <p>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。</p> <p>(二)規劃階段</p> <p>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。</p> <p>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：</p>	<p>三、系統開發生命週期 (SDLC) 管理</p> <p>(一)需求分析階段</p> <p>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。</p> <p>(二)規劃階段</p> <p>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。</p> <p>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：</p>	<p>一、配合實務作業需要，相關文件應於上線前提出，爰修正第四款第一目文字。</p> <p>二、配合資訊安全管理制度所依循之國際標準 ISO 27001:2013 版改版，強化本部資訊應用系統開發安全性，以符合安全系統開發生命週期(SSDLC)要求，爰新增第五款規定。</p>

<p>(1)系統功能架構圖。</p> <p>(2)系統流程圖。</p> <p>(3)系統環境需求說明文件。</p> <p>(4)需求變更明細表。</p> <p>(5)會談紀錄。</p> <p>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。</p> <p>(三)開發、變更與測試階段</p> <p>1、系統測試與開發環境，應與正式應用系統實體區隔。</p> <p>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。</p> <p>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。</p> <p>4、程式撰寫時應考量</p>	<p>(1)系統功能架構圖。</p> <p>(2)系統流程圖。</p> <p>(3)系統環境需求說明文件。</p> <p>(4)需求變更明細表。</p> <p>(5)會談紀錄。</p> <p>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</p> <p>(三)開發、變更與測試階段</p> <p>1、系統測試與開發環境，應與正式應用系統實體區隔。</p> <p>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。</p> <p>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。</p> <p>4、程式撰寫時應考量</p>	
--	---	--

<p>安全問題，避免出現已知之弱點。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>(四)上線階段</p> <p>1、系統相關文件，如使用者手冊、系統說明文件等，<u>應於系統上線前提出</u>。</p> <p>2、應用系統配合上線應辦理相關教育訓練。</p>	<p>安全問題，避免出現已知之弱點。</p> <p>5、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。</p> <p>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。</p> <p>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。</p> <p>(四)上線階段</p> <p>1、<u>應用系統上線時，應同時產出系統相關文件</u>，如使用者手冊、系統說明文件等。</p> <p>2、應用系統配合上線應辦理相關教育</p>	
---	---	--

<p>3、上線使用之應用系統時，應符合以下最低要求：</p> <p>(1)應用系統之密碼機制強度應符合本部相關規範。</p> <p>(2)應能明確建立權限劃分設定。</p> <p>(3)應能提供系統存取、帳號密碼變更之系統紀錄功能。</p> <p>(五)前述各階段均應同步以安全系統開發生命週期（SSDLC）進行安全檢核。</p>	<p>訓練。</p> <p>3、上線使用之應用系統時，應符合以下最低要求：</p> <p>(1)應用系統之密碼機制強度應符合本部相關規範。</p> <p>(2)應能明確建立權限劃分設定。</p> <p>(3)應能提供系統存取、帳號密碼變更之系統紀錄功能。</p>	
---	---	--