內政部消防署暨所屬機關系統開發及維護作業程序規範

一、目的

為建立內政部消防署（以下簡稱本署）暨所屬機關系統開發、維護之安全，特訂定本規範。

二、依據

（一）行政院及所屬各機關資訊安全管理要點。

（二）行政院及所屬各機關資訊安全管理規範。

（三）本署暨所屬機關資通安全政策及管理要點。

三、系統開發安全方針

（一）系統應依「資訊系統分級與資安防護基準作業規定」評定系統安全等級，並符合資安防護基準要求，相關要求得參考「資訊系統委外開發 RFP 資安需求範本」納入委外開發契約中。

（二）應用系統服務的資訊如使用於公眾網路上傳輸，應加以保護免於詐欺行為，契約爭議及未經授權的揭露與修改。

（三）如涉及重要資料之傳輸，應使用 SSL 加密金鑰，其金鑰並於生命週期妥善保護管理。

（四）系統測試與正式運作環境應予以分離。

（五）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。真實資料之複製情形應予以記錄，以供查考。

四、開發環境安全要求

（一）應避免使用可攜式電腦進行系統開發。

（二）開發用電腦應特別注意防止遭受惡意程式碼攻擊，以避免程式原始碼被感染或植入惡意程式碼。

（三）多人協作之開發環境其程式原始碼之存取權限應予控管。

（四）開發環境所使用之開發工具宜經過安全性確認，避免使用未經驗證或來源不明之工具程式進行開發。

五、安全系統設計原則

（一）具機密或個人隱私資訊之應用系統（AP），傳輸時應設計加密機制（如 SSL 或 https 等），必要時應針對資料內容加以保護，例如：資料庫加密，並記錄傳輸的相關資訊，包含傳輸來源、接收目的位址、傳送時間與傳輸成功或失敗等資訊。

（二）應視系統需求，進行會談期逾時（Session timeout）控制，以防止未經授權使用者的存取。

（三）輸入應用系統之資料，儘可能實施合理性檢查，以確保資料之正確與完整性。

（四）系統內部之處理作業宜建立檢核點或驗證資料正確性之作業程序，避免系統處理失誤。

（五） 作業系統或應用程式應安裝安全修補，以防止資訊系統的弱點被不當利用。

（六） 系統開發應避免將連線密碼直接明寫於程式碼中，且連線帳號應限制權限，避免使用最高權限帳號，例如：sa、root、admin 進行連線。

六、系統開發委外安全控管

（一） 於專案期間，應透過定期確認或稽核等方式監督委外廠商之資訊安全要求及個人資料保護之遵循情形；非經授權禁止於辦公處所外，遠端存取系統。

（二） 委外廠商進行系統開發、測試與維護時，未經權責主管許可，不得複製或攜出本署保有之密級或個人隱私資料。

七、系統變更與維護

（一） 系統變更時，應審查與測試系統，以確保無不利之衝擊。

（二） 系統（管理）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。

八、建構管理

（一） 系統開發人員應視需要產出系統相關文件，如系統分析報告、系統設計報告、程式規格書、測試計畫、測試報告及操作手冊等。

（二） 程式原始碼及執行碼應控管，並有版本控制機制。

九、附則

（一） 本署所屬機關得視本身業務之個別需求，依據本規範另訂相關規範，報署核備後實施。

（二） 本規範自核定後實施，修正者亦同。