

臺北市政府地政局介接使用數位印鑑比對系統 軟體委外廠商資訊安全稽核紀錄表

受稽核廠商：

稽核日期：

稽核項目	稽核結果	稽核情形
1. 資產安全		
(1) 專案文件管控含等級標示、保管、流通、通報與廢止等相關紀錄。	☐ 符合 ☐ 不符合 ☐ 不適用	
(2) 資產標示及管理紀錄。	☐ 符合 ☐ 不符合 ☐ 不適用	
(3) 專案資產清冊是否增列個資標示欄位，以資識別該項資產是否含有個資。	☐ 符合 ☐ 不符合 ☐ 不適用	
2. 人員安全		
(1) 專案人員是否簽署專案保密協定，並接受專案相關之資訊安全認知訓練紀錄。	☐ 符合 ☐ 不符合 ☐ 不適用	
(2) 查核是否依據專案工作內容妥善設置工作之代理人	☐ 符合 ☐ 不符合 ☐ 不適用	
(3) 查核專案人員及駐點人員是否於離開專案或合約終止時移轉所管理之專案資產。	☐ 符合 ☐ 不符合 ☐ 不適用	
(4) 查核期間專案人員異動時須調整或撤銷系統、網路、設備、門禁、文件及資料等使用權限，並留存調整或撤銷紀錄或表單。	☐ 符合 ☐ 不符合 ☐ 不適用	
3. 應用程式安全		
(1) 原始碼進行版本控制與存取控管，存取行為留下稽核日誌	☐ 符合 ☐ 不符合 ☐ 不適用	
(2) 程式開發測試區域，與正式上線環境需做區隔並做程式與軟體之版本管控	☐ 符合 ☐ 不符合 ☐ 不適用	
(3) 密碼設定需符合共用之密碼政策模組規定及應用系統使用者授權需透過「帳號授權模組」檢核	☐ 符合 ☐ 不符合 ☐ 不適用	
(4) 資料交換需將通訊資料加密	☐ 符合 ☐ 不符合 ☐ 不適用	

稽核項目	稽核結果	稽核情形
(5) 資料交換須保存完整的機敏資料新增、刪除、修改及讀取之稽核紀錄	☐ 符合 ☐ 不符合 ☐ 不適用	
(6) 應用程式修改更新時，須產生系統更新之紀錄，並確認系統相關文件是否依據程式修改更新	☐ 符合 ☐ 不符合 ☐ 不適用	
(7) 使用者透過專案網站上傳之檔案是否經加密處理並透過安全的傳輸協定傳輸	☐ 符合 ☐ 不符合 ☐ 不適用	
(8) 使用者透過專案網站上傳之檔案經系統接收後，是否自動執行掃毒程序，確認不含任何病毒後，才繼續執行後續處理	☐ 符合 ☐ 不符合 ☐ 不適用	
4. 系統及資料安全		
(1) 個人電腦是否安裝防毒軟體，並定期更新掃瞄引擎及病毒定義檔	☐ 符合 ☐ 不符合 ☐ 不適用	
(2) 查核個人電腦中有無安裝非專案所需之軟體	☐ 符合 ☐ 不符合 ☐ 不適用	
(3) 查核機敏資料傳輸，是否採行加密	☐ 符合 ☐ 不符合 ☐ 不適用	
(4) 查核專案帳號管理人員是否定期檢視帳號(含Superuser)與權限設定	☐ 符合 ☐ 不符合 ☐ 不適用	
(5) 查核系統開啟作業紀錄(Log File)是否記錄資訊安全事件	☐ 符合 ☐ 不符合 ☐ 不適用	
(6) 查核個人資料是否進行存取權限控管、資料加密、資料隱匿、資料存取稽核紀錄等方式加以保護	☐ 符合 ☐ 不符合 ☐ 不適用	
(7) 查核個人資料之存取是否經授權或申請核准，並記錄可辨識使用者之相關稽核軌跡	☐ 符合 ☐ 不符合 ☐ 不適用	
(8) 查核機敏資料是否使用相關保護機制，如：資料減縮、資料模糊化、資料隱瞞、資料擾亂、資料集成等方法，保護機碼資料安全性	☐ 符合 ☐ 不符合 ☐ 不適用	
(9) 現場查核設備時間是否正確使用NTP網路校時	☐ 符合 ☐ 不符合 ☐ 不適用	
(10) 查核應用程式、資料庫、主機、工作站、伺服器之稽核資訊是否自動整合至稽核管理系統	☐ 符合 ☐ 不符合 ☐ 不適用	

稽核項目	稽核結果	稽核情形
5. 實體安全		
(1) 實地查核機房是否實施門禁安全控管紀錄	☐ 符合 ☐ 不符合 ☐ 不適用	
(2) 實地查核廠商進入機房維修時，是否有專案人員派員監督	☐ 符合 ☐ 不符合 ☐ 不適用	
(3) 實地查核機房設置專用空調設備溫度是否保持攝氏20度至25度之間；相對濕度是否保持40至60之間	☐ 符合 ☐ 不符合 ☐ 不適用	
(4) 實地查核因業務需要將資訊設備攜出，是否完成設備攜出手續	☐ 符合 ☐ 不符合 ☐ 不適用	
(5) 實地查核外部攜入之設備是否符合資訊安全相關規定	☐ 符合 ☐ 不符合 ☐ 不適用	
6. 網路安全		
(1) 查核網路設備預設通行碼是否修改	☐ 符合 ☐ 不符合 ☐ 不適用	
(2) 查核系統是否依據系統申請使用IP位址、通信埠、Service服務類別進行設定	☐ 符合 ☐ 不符合 ☐ 不適用	
(3) 查核網路設備政策及存取清單(ACL)	☐ 符合 ☐ 不符合 ☐ 不適用	
(4) 檢視網路設備政策及存取清單(ACL)是否經核准後進行設定	☐ 符合 ☐ 不符合 ☐ 不適用	
(5) 檢視防火牆政策及存取清單(ACL)是否定期經專人檢視	☐ 符合 ☐ 不符合 ☐ 不適用	
7. 資安事件管理		
(1) 資訊安全事件通報查窗口及查核期間是否有發生系統資安事件，是否依據專案資安事件管理流程處理	☐ 符合 ☐ 不符合 ☐ 不適用	
8. 緊急應變		
(1) 查核是否擬定專案資安事件通報流程	☐ 符合 ☐ 不符合 ☐ 不適用	
(2) 查核是否明定專案代理人員及備援人力	☐ 符合 ☐ 不符合 ☐ 不適用	

稽核項目	稽核結果	稽核情形
(3) 查核是否完成定期備援測試計畫與演練計畫	☐ 符合 ☐ 不符合 ☐ 不適用	
(4) 查核是否辦理備援演練及確認應變演練紀錄是否正確	☐ 符合 ☐ 不符合 ☐ 不適用	
(5) 查核備援演練完畢後之結果是否檢討異常並進行事件分析	☐ 符合 ☐ 不符合 ☐ 不適用	
建議事項：		
稽核人員	受稽廠商代表	