資安需求

一、廠商應遵守「資通安全管理法及其施行細則與相關子法」、「行政院政府資訊作業委外安全參考指引」、「臺北市政府資通安全管理規定」及本局資訊安全管理系統（下稱 ISMS）各項資訊安全相關規範（以上皆已最新版為主），本局得視合約服務內容之需要，要求廠商提報資通安全保護措施及個人資料保護措施，本局並保留對廠商實施合約範圍內資通安全及個人資料管理檢查與稽核之權利，經檢查或稽核發現不符合本合約、規定或發現具有潛在風險，廠商應於接獲機關通知期限內改善。

二、廠商因承包及維護本專案相關系統運作，直接或間接獲得之個人資料及系統維護管理文件，應善盡保管及保密責任，並遵守「個人資料保護法」相關規定，非經機關或當事人同意，不得將獲得之全部（或部分）資料內容提供（或洩漏、銷售）給非執行本專案之公司員工或其他第三人，資料使用範圍亦僅限機關或當事人授權與本專案相關之服務事項，不得將獲得之全部（或部分）資料內容以各種形式媒體重製發行。

三、本專案相關機密資料，並應負保密責任、不得外洩，違者追究相關法律責任。

四、廠商應保證依本案所交付之工作成果與執行本案過程不得侵害他人之營業秘密、智慧財產權或其他權利，如因故意或過失不法侵害他人（含國內外自然人及法人）之營業秘密、智慧財產權或其他權利，廠商應負最終且完全之法律上責任。

五、廠商開發環境安全管理及教育訓練

(一)專案團隊每人接受 6 小時資安訓練（如公司自行舉辦資通及資通安全相關內部訓練等）。

(二)若機關需要前往廠商開發環境執行外稽時，廠商需配合接受稽核，並就稽核缺失依時限配合完全改善。

六、資訊系統設計

(一)禁止開放網頁瀏覽目錄權限，避免公務機密與個人資料外洩。

(二)應用系統設計應考量連線作業時間控制及操作逾時自動登出機制。

(三)錯誤及例外處理，發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細錯誤訊息。

(四)不得使用具風險之網頁資料傳送技術撰寫本專案相關程式。使用者之帳號及密碼不可以網址列參數方式傳輸。

(五)系統網站至少啟用 TLS1.2（含以上）加密連線機制，且禁止啟用低於 TLS1.0 含以下不安全協定；網站 SSL 憑證向機關資教科申請，並於維護期間檢視憑證之有效性。

(六)應用程式不允許有其他登入後門頁面。

(七)應用系統程式碼中與帳號密碼相關資料（如 webconfig 等）不允許明文。

(八)資料庫中密碼欄位不允許明文存放。

(九)若有上傳檔案功能，須以寫入資料庫方式為之，且上傳檔案須設白名單（如 JPG、PNG 及 PDF 等）。

(十)應用系統軟體更新應建立版本控管機制，並於正式上版前填寫機關 ISMS「正式作業變更管制紀錄表」。

(十一) 資料庫不允許使用 SA 帳號連結（SA 帳號僅管理帳號使用），資料庫帳號應以最小原則化開設權限。

(十二) 資訊系統應符合「資通安全責任等級分級辦法」附表九資通系統防護需求

分級原則進行分級，相關功能應符合附表十防護基準之要求。

七、系統存取控制

(一)使用者第一次使用應用系統時，應更新初始密碼後方可繼續作業。

(二)對於使用者忘記密碼之處理，應有身分確認程序，方可再次使用系統。

(三)依應用系統特性限定其作業時間，以減少未經授權人員存取系統之機會。

(四)系統通行密碼長度至少 8 碼（建議為 12 碼），並應由大寫字母、小寫字母、數字三種組成。

(五)提供系統帳號密碼強制使用者更新機制。

(六)系統帳號連續 1 年無登入紀錄，將該帳號停用，並設計帳號恢復機制。

(七)廠商禁止使用共用帳號（如廠商 2 名應建立 2 組帳號）。

(八)系統應有安全身分鑑別及防止暴力破解帳號密碼機制（如圖形驗證等）。

(九)允許使用者自行選擇及更改通行密碼機制。

(十)使用者之密碼應與應用系統資料分開存放並加密處理。

八、稽核存錄

(一)系統須有使用功能權限及資料庫存取管制功能，識別使用者身分，防止非合法授權人員進入使用，並於進行認證授權時，系統需提供相關軌跡紀錄（LOG）系統使用情形（欄位起碼包括使用者帳號、來源 IP、登入日期）。

(二)資訊系統作業中斷及更正等異常事項，應記錄 LOG 檔。

九、個人資料保護

(一)應依據「個人資料保護法及其施行細則」等相關規定，審慎處理及保護個人資訊。

(二)廠商僅得為辦理本合約所載委外業務之相關目的，蒐集、處理、利用或傳輸個人資料，並符合「個人資料保護法及其施行細則」、本局所訂定個資保護相關程序規範及其他相關法規命令。

(三)資訊系統應合理留存個人資料之新增、修改、刪除、資料匯出、列印等活動之操作紀錄。

(四)處理含個人資料之資訊系統，除執行業務所必要者外，應避免提供資料整批匯出功能，以資料最小原則化需求為主，且資料若含個資，應去識別化（視機關實際作業需求調整）。

(五)測試資料應避免使用含有真實個人資料（正式資料）資料庫進行測試；如須應用真實資料，應於事前刪除足以辨識個人之資料並採取適當之安全保護措施。

(六)刪除及修改個資欄位動作，系統需設計複核機制，且留存刪除資料。

十、資料備份備援

(一)廠商須針對系統程式、資料庫及使用者資料之損毀、遭外力破壞等可能影響本專案各項服務正常運作之情形，提出完整之資料備份建議及系統備援方案，並依標準程序操作實施。

(二)視機關需求辦理災難復原演練（BCP）及資料備份備援計畫（機關核心資通系統必須辦理）。

(三)資料庫備份檔（如.BAK 等）需加密。

十一、　應用系統漏洞檢測

(一)使用第三方元件需提出使用合法證明，若有過時或漏洞元件需於完成修改。

(二)系統上線前應配合機關主機弱掃、網頁弱掃或滲透測試或原碼檢測報告時程修改系統漏洞（若機關無提供則本條不適用），「中級以上」及「判定為 SQL

Injection及Cross Site Scripting之低風險」應全數修正完畢，並填寫機關提供之市府ISMS「臺北市政府資訊局弱點掃描處理情形回復表」。

(三)如發生資安事件，廠商需無償修復至完成相關檢測漏洞，並即時通報機關資安人員（若事件因廠商端發生得負連帶賠償之責任)。