桃園市政府資訊服務採購 RFP 資通安全範本

壹、前言

一、公共工程委員會（PCC）於 112 年 9 月 25 日函頒《**政府資訊服務採購作業指引**》，明定「資訊服務採購契約範本」之適用範圍，並附「**各類資訊(服務)採購之共通性資通安全基本要求參考一覽表**」作為最低資通安全門檻。

二、本府各機關辦理資訊**系統建置、系統維運、設備採購或設備維運**等案，應先行參考以上兩項中央文件，於採購時使用「資訊服務採購契約範本」，並遵循契約範本內所列資安條款，避免使用勞務採購、財務採購等其他契約範本。

三、本文件僅屬輔助範例，並**不取代中央契約範本。若本範本與中央最新規定牴觸，以中央規定優先**。

四、請各機關在擬定 RFP 及契約時，充分**考量自身系統的規模、關鍵性及風險等級**，在範本的基礎上進行適度的客製化，如時程、違約計點及罰則的具體數值。

貳、目的

提升本府及所屬機關資訊系統之資通安全防護水準，確保採購案在系統建置、維運、設備管理與開發過程符合資安要求，並對得標廠商之義務加以明確規範，本文件供各機關辦理徵求建議書（RFP）及契約附件擬定時參據。

參、適用範圍

本規範適用於本府及所屬機關辦理與資訊服務相關之採購案件，包含但不限於：

一、資訊系統建置專案。

二、系統維運與維護服務。

三、設備採購與汰換處理。

四、委外系統開發與管理。

肆、法規與參考基準

本規範之制定與廠商資安義務之要求，係參照並依據以下主要法規與參考基準，確保本府資訊服務採購符合國家資通安全政策與要求：

一、《資通安全管理法》：主要規範資安事件通報、弱點管理、委外廠商監督及相關罰則，旨在建立資安治理體系，提升資安防護及應變能力。

二、《資通安全責任等級分級辦法》附表十資通系統防護基準：針對不同資通系統防護需求等級規範控制措施，包含漏洞修補、資安健檢等要求。

三、公共工程委員會《政府資訊服務採購作業指引》：明定政府資訊服務採購應採用「資訊服務採購契約範本」，並將「各類資訊(服務)採購之共通性資通安全基本要求參考一覽表」作為資通安全最低門檻。

四、數位發展部資通安全署《資通系統籌獲各階段資安強化措施》：明定機關依《資通安全管理法施行細則》第四條規定選任或監督受託者之相關行政流程及應注意事項，並將「資訊服務採購案之資安檢核事項」及「廠商資安管理作業自我評估表」供各機關辦理資訊服務採購時參據。

五、國家資通安全研究院《政府資訊作業委外資安參考指引》：針對不同類型之資訊委外各階段應注意之資安事項提供參考指引，並提供「Web 應用程式安全檢核表」供各機關辦理 Web 應用程式委外開發時，依據系統的安全強度，要求廠商(或第三方)執行不同程度的檢核。

六、國家資通安全研究院《資通系統防護基準驗證實務》：針對資通系統防護基準，逐項說明各項控制措施之內容說明及驗證實務，並提供可能之佐證資料作為驗證之參考依據。

伍、資訊服務採購契約及資安指標服務水準（SLA）

為確保資訊服務供應商（廠商）能持續提供符合資安要求的服務，特訂定「桃園市政府資訊服務採購契約範本機關資安檢核表」(如附件 1)資訊服務採購契約範本以下。各機關應依個案特性，在契約中明確載明各項資安要求項目、資安指標服務水準（SLA）違約計點原則及「○點」之具體數值與相關罰則，違約金金額應本於契約誠信原則與比例原則，與契約總價相稱。以維持履約壓力之公平性及實務執行之正當性（例如，小額採購案可酌減罰鍰標準，大額採購案亦得適度調整罰鍰上限，以維持合理之履約壓力與公平性）。

陸、系統建置階段資通安全規範

為確保所建置資訊系統之資通安全，廠商於開發與建置過程中應遵守以下規範：

一、 本案履約涉及之資通系統，其防護需求等級為 □普級、□中級、□高級，其資通安全基本要求工作事項應依資通安全責任等級分級辦法附表十「資通系統防護基準」要求之□普級、□中級、□高級 各項控制措施辦理。

二、 **測試環境使用**：所有測試資料和程式檔案應於測試系統或環境上使用及測試，測試確認無誤後才能移至正式環境或上線。廠商於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。

三、 **版本控制**：程式碼應進行版本控制（如 Git、SVN、Azure DevOps Server 等），確保開發過程可追溯與管理。

四、 **安全開發**：

(一)系統應避免顯示原始錯誤訊息（如 SQL 語法、版本資訊），發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息，並強化資料輸入驗證及存取控制機制，防止惡意輸入或繞過身分驗證機制存取未經授權之內容。

(二)系統應依最新穩定版 OWASP Top 10 應用程式安全風險要求與本府資訊安全政策開發，並落實應用系統資安檢測及漏洞修補，不得有最新版 OWASP Top 10 等之資通安全弱點。

五、 **攻擊防範與檢測**：網頁應用系統應能有效防止常見資安攻擊（如：XSS、SQL Injection 等），並於驗收前提交第三方資安檢測報告（如弱點掃描、滲透測試、源碼掃描結果與修補狀況）。

六、 **漏洞修補後上線**：若檢測發現中、高風險漏洞，需修補完成並複測確認安全無虞後才可上線。

七、 **安全傳輸協定**：資通系統傳輸應採用 HTTPS（透過 TLS 1.2 以上等加密協定）協定，以確保資料以密文方式傳輸。

八、 **開源/第三方軟體管理**：為強化系統交付品質與安全，廠商於開發與建置階段，即應落實所用之開源軟體或第三方軟體元件之版本更新與風險修補，並定期掃描其資安弱點。涉及利用非受託者自行開發之系統或資源者，應標示非自行開發之內容與其來源及提供授權證明，並於驗收前提交機關。相關義務及罰則比照維運階段之資安規範辦理。

柒、系統維運階段資通安全規範

廠商於系統維運階段，應確保系統之穩定運行與資通安全，並履行以下義務：

一、定期維護、弱點修補與更新管理：

(一)本案履約涉及之資通系統，其防護需求等級為 □普級、□中級、□高級，其資通安全基本要求工作事項應依資通安全責任等級分級辦法附表十「資通系統防護基準」要求之□普級、□中級、□高級 各項控制措施辦理。廠商應定期辦理資通系統維運作業並將執行紀錄（如：帳號盤點、帳戶鎖定原則及密碼原則檢視、帳號登入及異常日誌檢視、系統源碼與資料備份、效能調校、主機環境資源檢視及系統版本更新等）交付機關，供機關確認資通系統維運作業確實依資安管理措施落實辦理。

(二)廠商應每年配合辦理弱點掃描及其他安全性檢測，並於檢測出風險後依機關要求期限完成中、高風險弱點修補並提出改善報告，經 2 次複測未改善者，視為違約。

(三)廠商應依最新作業系統公告進行 Service Pack 與 HotFix 等修補，為無償作業，並應留存修補紀錄並交付機關查核。

(四)廠商應主動更新病毒碼、防毒機制；雲端硬碟、網路附加儲存（NAS）等設備，應定期進行掃毒作業。

(五)廠商應主動依原廠公告與風險評估結果，定期更新系統相關軟體（如作業系統、中介軟體、應用程式、防毒碼等），並應就已部署之更新保留紀錄並交付機關查核。軟體更新之修補時程，應依資安風險等級（高、中、低）比照弱點修補作業，於合理期間內完成。

(六)廠商應避免因自動更新造成服務中斷或版本相容問題。重大變更前，應與機關協調並進行測試，確認不影響既有功能與資安設定。

(七)未依機關要求期限完成修補或更新者，經通知後仍未改善，機關得依契約向廠商每次處以違約金。

(八)因延遲修補或更新導致實際資安事件或服務中斷者，機關得依契約向廠商追償實際損害。

(九)累計三次以上未依規定更新者，視為重大違約，得提前終止契約。

二、日誌與監控：

(一)網站主機、資料庫等應具備日誌、告警、帳號異常行為(如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、

功能錯誤及管理者行為)記錄機制，並保留至少 6 個月之稽核紀錄，供機關查核。

(二)對日誌紀錄進行適當保護及備份，避免未經授權存取或竄改。

三、**帳號、存取與資料保護：**

(一)廠商應確保系統帳號不得共用，應用系統、伺服主機、作業系統、資料庫等皆不得使用預設帳號或弱密碼。應實施角色分級權限管理，並要求使用符合密碼複雜度要求之高強度密碼。

(二)系統應具備使用者識別與存取控制機制，並符合資料傳輸加密標準（如 TLS 1.2 以上，LDAPS 與 128bit 金鑰等）。

四、**法規遵循與人員管理：**

(一)廠商應遵守個人資料保護法、資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守機關資通安全管理及保密相關規定。建議提供符合 ISO 27001(ISMS)等國際資安管理標準之證明或說明其內部管理程序如何符合相關原則，並與機關簽署保密協定。

(二)履約人員不得於本府網路執行與業務無關之操作，亦不得擅自攜出設備。所使用軟體需為合法授權。廠商應確保所有參與本案之履約人員，定期接受資安教育訓練，提升其資安意識與專業能力。

五、**資安事件管理與通報：**

(一)若因未即時修補或更新導致資安事件，廠商應於事件發生後1小時內通知機關（或接獲機關通知1小時內），並採取適當之應變措施（提出處置計畫），並於 72 小時(重大資安事件為 36 小時)內完成損害控制或復原作業（如完成臨時修補或進行系統隔離作業），最終應於 1 個月內提交事故調查、處理及預防改善報告（或協助機關調查處理）。(**各機關應根據系統之關鍵性與資安風險評估，於招標時明確訂定上述時程，且時程不得低於資安法要求**。)

(二)應建立異常處理標準作業程序（SOP），並於事件發生時立即回報並配合調查。廠商宜於契約簽訂後一定時間內，提交此 SOP 供機關審閱，確保其程序符合機關要求且具備可行性。

(三)廠商應指定專責資安聯繫窗口，並與機關建立明確之資安事件緊急通報途徑與機制，確保資安事件發生時能高效溝通與協處。

捌、設備維護與管理資安規範

一、廠商應每季針對所有硬體設備進行安全健檢及維護紀錄，包括功能檢測、登入紀錄查核、異常行為告警等。

二、關鍵設備故障時，須於上班時間 4 小時內到場，並於 8 小時內修復或提供同等級備品替用。

三、設備維護人員須簽署保密同意書及保密切結書，並遵守機關規範，不得未經授權連接或使用任何非機關核准之設備或外部媒體（如 USB、行動硬碟等）。

玖、設備汰換或新購資安規範

一、新購設備應優先選用具資安認證產品，並符合政府公告或國際標準。例如，可優先考量具備 Common Criteria（ISO 15408）或 FIPS 140-2 等產品資安認證之產品，確保設備之安全性。

二、設備報廢應完成以下作業：

(一)硬碟抹除或物理毀損（如粉碎等），確保資料無法復原。

(二)清除作業系統與所有帳號設定，回復至出廠預設狀態。

(三)凡涉及個人資料、機密資料或帳號密碼等敏感資訊之設備，其汰換或報廢作業應留存詳細紀錄至少三年備查。

三、 應確實填具報廢與銷毀紀錄，並由機關人員全程監督錄影佐證，以確保作業符合規範。

壹拾、其他補充事項

一、**委外管理責任**：廠商如委外執行上述資安相關工作，應於契約中明確訂定其分包單位之資安責任與義務。該分包單位應一併納入機關或廠商之稽核對象，並要求廠商提供對分包單位之稽核計畫、頻率、方式（如書面審查或現場查核）及稽核報告，以確保其資安管控能力。

二、若廠商違反本規範或涉及違法情事，廠商應負全部責任，機關得依契約條款向廠商追償所有損害。

三、本規範應納入採購契約附件，並作為履約審查與驗收之重要依據之一。

四、機關辦理資訊服務採購時，應填具附件1「桃園市政府資訊服務採購契約範本機關資安檢核表」進行自我檢核，並應將附件 2「桃園市政府廠商資安管理作業自我評估表」列入招標文件供投標廠商依規定填妥後於投標時提供各機關參據。