財團法人中華民國對外貿易發展協會

場館營運系統

招標案

（案號: 2022K0051054）

服務建議徵求書

(Request for Proposal)

中華民國111年12月

目　　　　　錄

[壹、 專案說明 3](#_Toc120867826)

[貳、 專案需求 4](#_Toc120867833)

[參、 專案組織 5](#_Toc120867834)

[肆、 專案管理 5](#_Toc120867835)

[伍、 驗收事項與交付文件 5](#_Toc120867836)

[陸、 保固與維護方式 9](#_Toc120867840)

[柒、 服務建議書製作規定 12](#_Toc120867841)

[捌、 評選決標事宜 12](#_Toc120867848)

[玖、 庶務事項及其他 13](#_Toc120867849)

[壹拾、附件清單： 13](#_Toc120867860)

# 專案說明

1. 專案名稱

財團法人中華民國對外貿易發展協會（以下簡稱本會）「場館營運系統招標案」（以下簡稱本專案）。

1. 專案目標

本專案為針對本會經營之展覽暨會議場館例行維運管理需求，所建置之營運管理系統，適用範圍須涵蓋現有世貿中心、南港一館、南港二館、會議中心，並可擴充於未來其他展館，滿足實體場地出租業務相關作業與管理需求。活動主辦單位自檔期洽訂、租用/變更展場及會議室空間、活動辦理相關資源調度/通報等作業，結合訂單之報價試算、簽約與付款、費用結算等，並提供多角度管理統計報表與營運數據(預算、營收、收益)分析，以便精準掌握各硬體單位之營運狀況，達成永續經營的目標。

1. 專案範圍

專案需求範圍如下：

1. 場館營運系統建置（含UI/UX設計、程式設計開發與資料介接）、安裝、測試與上線等工作。
2. 場館營運系統規劃之功能模組細部設計文件，應於教育訓練中說明，並提供相關諮詢。
3. 場館營運系統之技術移轉，應涵蓋軟體開發、維護、設備基礎建設、資訊安全等內容，並提供技術移轉輔導，技術移轉輔導內容須涵蓋軟體開發、維護、基礎建設、資訊安全團隊等範圍（總時數應安排至少 5 個人天以上）。
4. 依場館營運系統之功能模組提出雛型展示規劃。
5. 場館營運系統之舊資料移轉，應涵蓋現有四個單位(世貿中心、南港一館、南港二館、會議中心)使用之營運系統，其資料須移轉至本專案新建置之系統上，並提供資料上線移轉計畫。
6. 場館營運系統保固 1 年，應包含維運及相關諮詢工作。
7. 專案時程

本專案總執行時間共 18 個月，得標廠商需自簽約日起，18個月內完成本專案之整體驗收作業。

得標廠商須自簽約日起 1 個月內完成本案第一期工作項目，包含專案導入時程計畫書(SOW)；於簽約日起 6 個月內完成第二期工作項目，包含系統分析及系統設計；於簽約日起 16 個月內完成第三期工作項目，包含系統建置及測試驗收；自簽約日起 18 個月內完成第四期工作項目，包含教育訓練及技術移轉。於專案驗收後，提供 1 年保固、維護及技術諮詢服務。

1. 主辦單位

本專案主辦單位：財團法人中華民國對外貿易發展協會

專案聯繫資料如下：

1. 本會地址：台北市基隆路一段333號國貿大樓7樓
2. 聯絡人： 呂婕瑜
3. 電話：02-27255200 ext. 1743
4. 傳真：02-27576245
5. 電子信箱：[shalinlu@taitra.org.tw](mailto:shalinlu@taitra.org.tw)
6. 專案經費

本專案應用系統開發經費為新臺幣 1,000 萬元整(含稅)。本案場館營運系統，於保固維護期間將進行本會例行之資安檢測相關作業，若發現存在資安風險之漏洞，得標廠商應無償進行漏洞修補。如完成程式漏洞修補後再進行複測，仍有漏洞未完成修補而產生之額外檢測等費用，廠商應負責支付該筆費用。

# 專案需求

本專案詳細需求如「需求說明書」（附件一）所列。若得標廠商所提建議書有優於本專案招標文件之處，經本會同意者，從其優者。

廠商可於所提建議書及簡報中，就本建議書徵求文件規定事項，以及需要本會配合辦理之事項提出建議意見。得標廠商提出之建議意見，經評選委員會決議採納並作成紀錄者，其效力優於本需求文件。

# 專案組織

廠商須就本專案建置與維運服務期間，分別指派專職人員負責本專案相關工作之推動，並於建議書中詳述組織、分工與職掌等事宜。有關本專案技能要求如下：

* 廠商本案參與人員應具有相關方面專業證照，如：Java軟體原廠認證SCJP及SCWCD或.NET軟體原廠認證MCSD/MCAD等，並於建議書中詳細說明。
* 廠商本專案經理須具備五年以上相關工作經驗。建議書應附參與本專案人員履歷表及相關佐證資料。

# 專案管理

本專案執行須依本會「專案管理方法說明」執行，本案採混合式專案管理(Hybrid Agile)方式進行。得標廠商須提出專案工作計畫書，於議價簽約後7個工作天內，依據建議書與評選簡報時之承諾、評選委員會之決議，配合本會意見修改本案企劃書，並依照本文件描述各專案階段執行。專案工作計畫書內容應包括對本專案之執行敘述，包含專案管理、工作項目、時程、進度稽核點、品質管控，以及本會配合事項等。

# 驗收事項與交付文件

1. 交付項目：

本專案之各驗收階段的時程與交付項目，除專案系統開發之產出外，亦須包含其他工作事項。例如：資料介接、教育訓練、技術輔導等。各階段交付項目列表，須依本會「專案委外開發管理方法說明–第七項：交付項目列表（專案分級：大型專案）」所述交付。列出如下：

|  |  |
| --- | --- |
| 工作階段 | 交付項目 |
| 1. 專案啟動階段 | 專案導入時程計畫書(SOW)  會議記錄  專案工作計畫書(WBS)  系統分析說明書範本 (請見\*文件規範說明)  程式設計說明書範本 |
| 1. 需求分析階段 | 需求訪談紀錄  需求規格書  系統分析說明書  線框稿(Wireframe)文件  需求垂直追溯表 |
| 1. 雛型設計階段 | 系統雛型文件 |
| 1. 技術設計階段 | 程式設計規格書  系統架構規格書  資料庫規格書  需求垂直追溯表(更新版)  資料移轉規劃及設計 |
| 1. 程式撰寫與功能測試階段(Unit Test) | 分階段雛型展示：於系統分析與系統設計(預定第6個月完成)後，每2個月進行功能雛型展示  功能開發時程管控表  版本控制方法說明  資料移轉程式撰寫  功能測試個案計畫書  功能測試個案報告書 |
| 1. 整合測試階段  (System Integration Test) | 整合測試計畫書 (含測試案例及資料移轉案例)  整合測試報告書 |
| 1. 使用者測試階段  (User Acceptance Test) | 使用者測試計畫書  使用者測試報告書  資訊安全及壓力測試計畫書  資訊安全及壓力測試報告書  系統上線計畫書 |
| 1. 驗收階段 | 驗收清單  教育訓練計畫書  使用者操作手冊  安裝手冊  系統維運手冊  系統架構規格書（最後更新版）  資料庫規格書（最後更新版）  程式規格書（最後更新版）  應用程式原始碼（最後更新版）  相關軟體智慧財產權證明文件 |

\*系統分析說明書範本-文件規範說明：請廠商依功能觀點、物件觀點、動態觀點提供對應之UML文件，如下列UML Diagrams

1. Use Case模組或流程使用案例
2. 活動圖(Activity Diagram)
3. 循序圖(Sequence Diagram)
4. 狀態圖(State Diagram)
5. 簽核流程圖及說明
6. 專案查核與罰則
7. 規定各階段交付項目交付時間，若廠商未按規定時間交付，或文件章節格式未符合本文件規定，予以計罰。
8. 規定廠商之回覆期限，對於本會之書面提問或於專案資訊網站之提問，若廠商未按時限回覆，予以計罰。
9. 廠商提交需求規格書初版時，若有漏列「服務建議徵求書」或「需求訪談」所敘述之需求，予以計罰。
10. 上述項目，廠商交付遲延時，每逾一日，應按契約報酬總額之千分之 3 計付違約金，本會得逕自應給付之契約報酬中扣除，違約金上限為本合約服務費總價 20% 。若達上限，本會得逕自解除契約，廠商所繳納之保證金不予發還。 各專案工作項目如有階段性之時程需求，請依本專案相關之規定完成。
11. 針對廠商交付確認之功能測試、整合測試，本會將進行重複測試，若發生測試項目「失敗率」超過已完成測試項目 30% 情事，甲方即不再進行測試，請廠商重新驗證系統品質。因品質所造成專案時程延遲，將加重違約金，按契約報酬總額之千分之 4 計付違約金。
12. 分期付款方式配合各階段產出項目之審核，通過審核列為各期付款條件。
13. 驗收及付款：
14. 驗收：
    * + 1. 廠商應分別於各期工作完成後，以書面通知本會審查、確認與驗收，並交付相關文件；如審查結果有需改正項目，廠商應於 2 週內完成改正，並以書面通知本會辦理複審及確認。
        2. 得標廠商應於簽約後，依本專案階段完成驗收；若因不可抗力事故造成履行遲延或中斷逾 20 個工作日時，除非雙方當事人另以書面達成協議，否則甲方得以書面通知廠商終止契約。
        3. 在品質認定上，得標廠商須以本會要求之品質為認定依據，如無法達成要求，本會可退回驗收之項目，限期改善。
15. 付款：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 階段 | 專案委外開發管理方法說明所定義階段 | 付款金額 | 付款條件 | 付款方式 |
| 第1期  (自簽約日起1個月) | 1. 專案啟動階段 | 佔總價款10% | 交付所有項目，經本會審查通過。 | 備妥各項交付文件及紀錄送本會辦理驗收。 |
| 第2期  (自簽約日起6個月) | 1. 需求分析階段 2. Wireframe設計階段 3. 雛型設計階段 4. 資料移轉規劃 5. 技術設計階段 6. 第2期驗收 | 佔總價款25% | 交付所有項目，經本會審查通過。 | 備妥各項交付文件及紀錄送本會辦理驗收。 |
| 第3期  (自簽約日起16個月) | 1. 程式撰寫與功能測試階段 2. 整合測試階段 3. 使用者測試階段 4. 功能個案測試階段 5. 資料移轉階段 6. 第3期驗收 | 佔總價款45% | 交付所有項目，經本會審查通過。 | 備妥各項交付文件及紀錄送本會辦理驗收。 |
| 第4期  (自簽約日起18個月) | 1. 教育訓練及技術移轉輔導 2. 系統總驗收 | 佔總價款20% | 交付所有項目，經本會審查通過。 | 備妥各項交付文件及紀錄送本會辦理驗收。 |

# 保固與維護方式

1. 本專案免費保固範圍為本專案之全部範圍，免費保固維護期為驗收完成日起 1 年。
2. 得標廠商於保固期過後，仍需負系統之維護責任。於保固期滿前 3 個月內，雙方需簽訂軟體維護契約，維護費用以每年不超過本案總經費 13% 為限，維護範圍包括因應個人電腦作業系統暨瀏覽器版本變遷時相關元件所需之升級、資安檢測弱點修補、回答使用者詢問、檢視系統報告、備援演練，及修復系統問題。
3. 本會將每年對於本合約標的物（含應用程式與行動應用App如 iOS、Android等）進行資訊安全檢測，包括網頁弱點掃瞄、主機弱點掃瞄、滲透測試，本會將於檢測後通知廠商檢測結果，廠商應於接獲通知三周內完成檢測弱點修補或強化。本會將於通知後三週進行第2次檢測，若仍有發現弱點，廠商應於第2次檢測三周內完成弱點修補或強化；本會將於通知後三週進行第3次檢測，第三次檢測費用由廠商負擔，第三次檢測如發現仍未修補，以廠商違約論處；另廠商之修補應配合填寫本會之弱點修補紀錄與系統異動表單。
4. 廠商執行本合約發現任何資安事件，應於發現後半小時內通知本會，並視事件嚴重程度採取合宜因應措施。
5. 廠商所提供之服務，如需調整、修補軟體，需遵循本會作業規定，以本會所屬之Github對原始碼進行版本管理。並確保Github資料與甲方變更管理紀錄一致。變更管理紀錄應遵循甲方ISMS相關規範格式。
6. 本會得訪查廠商就本合約範圍內提供之服務與環境，並得委由專業第三方進行稽核；廠商應依本會要求提供書面資料或配合實地稽核邀集相關人員參與。如經本會提出書面缺失廠商應限期改善，如無正當理由拒絕稽核或未依限改善，本會得以違約論處。
7. 本會得要求廠商對本合約標的物之異動提供原始程式碼檢測（源碼檢測）或要求廠商配合甲方源碼檢測作業，依本會要求項目與進度期程完成修補並配合填寫相關紀錄表單。
8. 本專案相關維護作業配合事項：
9. 回應時限：
   * + 1. A級：系統服務中斷
10. 報修回應與修復時間：每週7天每天24小時。
11. 廠商專責人員應於接獲甲方維護請求後2個小時內提出可行之解決方案回覆，並於4小時內讓系統恢復正常運作。
    * + 1. B級：系統功能障礙
12. 報修回應與修復時間：每週5天每天8小時，修復時間為正常上班時間內（週一至週五上午八時至下午六時）。
13. 廠商專責人員應於接獲甲方維護請求後4個工作小時內提出可行之解決方案回覆，並於1個工作天內讓系統恢復正常運作。
    * + 1. C級：系統需求變更
14. 廠商進行變更作業時須按甲方指定時間與方式進行，且變更後須提交上版異動紀錄表。
15. 廠商於系統進行變更作業前須填具甲方「ISMS-D60資通系統異動申請單」申請後進行變更，並須填報甲方所規定之系統維運文件並提交與甲方查核。
    * + 1. 其他問題：一般使用上問題需於1個工作天內回覆，系統性問題需詢問相關人員者於2個工作天內回覆。
16. 維護作業
    * + 1. 例行性事務
17. 廠商主動每月派員進行系統檢測、整理主機資料、清除歷史紀錄，並提供每期委外維護紀錄表與相關書面報告予甲方。
18. 廠商須提供應用軟體及相關技術之諮詢服務與建議方案。
    * + 1. 事件處理

廠商應提供符合甲方所提出應用系統維護處理工作需求服務，項目包括：

1. 系統服務中斷處理。
2. 系統功能障礙或異常處理。
3. 應用程式除錯。
4. 事故若判定為硬體故障時，須提供相關判定之訊息。
5. 應用系統所使用之程式相關資料庫操作（如：資料表操作、Trigger、Store Procedure、View、例行作業排程、資料異動）調整與維護。
6. 相關系統設定組態之保存，程式原始碼之保存與交付。
7. 每季資安稽核需交付相關文件。
8. 災難發生或硬體更換時，負責軟體之移置、回存、調整，或重新安裝（含作業系統、相關軟體元件及應用程式）與提供復原計畫。
9. 若無法以遠端連線進行維護，則須赴系統實體位置進行維護。
   * + 1. 一般諮詢：無須記錄之非書面諮詢，不列入回應時限。
10. 資料備份與還原
    * + 1. 應用系統資料應備份，範圍涵蓋：一般性應用資料、系統性資料（如組態、設定檔、密碼檔、程式檔等）以及稽核紀錄檔。
        2. 資料備份：需每日進行一次完整備份。
        3. 資料損毀與還原：當發生資料損毀事故時廠商需即時通知甲方，若發現者為甲方，則廠商於接獲甲方通知後需立即進行資料還原作業，依本會規定資料損失時間最多以24小時為限。若發生甲廠商不可控之外力（如：自然災害、電力供應問題、雲端服務中斷等），廠商評估恢復時間需時超過期限，應提出方案與甲方討論並確認完成日期。
11. 關鍵績效指標（KPI）

本專案驗收時，廠商依本案需求所開發之系統，必須達成本文件所列之各項KPI，如未達標則必須排除系統相關問題。除必須達成之各項KPI外，並請於建議書中詳列本專案所能提供或其他未列於文件中之各項關鍵績效指標（KPI），做為審標及將來驗收依據並明訂為合約履約項目。

|  |  |  |
| --- | --- | --- |
| KPI項目 | 項目描述 | 標準 |
| 系統可運作時間 | 除系統定期維護外，系統可運作的時間 | 99% |
| 系統同時上線人數 | 系統同時間可以正常服務的有效登入使用者會話(User Session)數量。 | 至少150人 |
| 系統回應時間 | 係指當系統收到使用者所發出之HTTP請求，產生HTTP回應到使用者端的時間(不包含網路傳輸時間)。 | 低於3秒 |
| 網頁渲染時間 | 在瀏覽器接收到網頁資源後可以正常顯示給使用者的時間。 | 低於1秒 |
| 其它關鍵績效指標 | 請詳列於建議書 |  |

# 服務建議書製作規定

1. 廠商應以精簡扼要、逐條直接回覆服務建議徵求書項目之方式撰寫建議書內容，以利本會掌握建議書之重點。
2. 建議書內頁應包括：封面、目錄、編頁碼、內文；內文篇幅以50頁為上限。
3. 請以紙本方式製作服務建議書，A4之紙張直式橫寫製作，並以電腦繕打；文字以橫排方式編排並編頁碼；並於左側裝訂牢固。
4. 服務建議書裝訂後，如有缺漏、錯誤或須補充部分，須製作勘誤表或補充說明。
5. 建議書應檢附一式十份，其中一份建議書，封面應註明「場館營運系統」及「投標廠商名稱」之字樣；請加蓋廠商及負責人印鑑，並蓋騎縫章，其餘九份得免蓋。
6. 建議書目錄大綱詳如附件二。

# 評選決標事宜

本案依採購法第22條第1項第9款規定，採限制性招標以公告程序委託專業服務、技術服務或資訊服務，經公開客觀評選為優勝者。本會將邀集學者專家及會內人員組成評選委員會，進行服務建議書之評選，投標廠商資格請另詳「投標須知」及「投標廠商聲明書」之規定，評選流程詳「評選須知」。

# 庶務事項及其他

1. 投標廠商在評選會議上所作之承諾應以書面列入合約附件中。
2. 本文件及相關之需求附件於決標後列入合約附件中。
3. 投標廠商在本專案中，整合使用其他廠商所發展之軟體產品，應詳列開發廠商及軟體產品名稱，並由承包廠商切結負責相關著作權問題。
4. 專案進行期間，廠商須就本專案相關事項與本會進行協商、說明、報告、簡報等，均須指派參與本專案之專案小組負責人或專案經理出面行之。
5. 得標廠商須提出負責本專案各功能子系統之技術人員聯絡窗口，隨時與本會以電話、E-Mail 對各功能開發需求進行溝通確認，並至少每兩個星期召開一次會議，討論專案規畫、開發、維運及專案文件等相關問題。
6. 得標廠商於系統開發期間所建立系統發展標準規範須經本會同意後施行。
7. 本系統結案時需交付開發程式原始碼，系統開發過程使用之元件，若為自行開發者，亦需交付原始碼。若該元件為購自其他公司者，需於結案時交付採購證明。使用自由軟體（Freeware）之元件，應交付原始碼或提出相關測試證明，並納入系統維護範圍，以確保元件之安全性及可用性，不得以任何理由拒絕後續維護。
8. 得標廠商在計畫期間，有接受有關本計畫工作諮詢之義務，在計畫方法錯誤、資料過時、或內容空泛等正當情形下，得標廠商應充分配合修正增補部分計畫內容，並不得要求增列額外預算。
9. 本案開發應採行CMMI精神發展，並以採行跨平台元件技術開發者為佳。
10. 投標廠商於其服務建議書中提供之報價單不宜註記與總金額數字不符之協議價」或「優惠價」，以致無法判斷個別項次之單價金額。

# 附件清單：

1. 附件一：需求說明書
2. 附件二：線框稿示意圖
3. 附件三：軟硬體、技術規格及資安需求 (請見本章內容)
4. 附件四：系統移轉需求 (請見本章內容)
5. 附件五：建議書大綱 (請見本章內容)

# 附件一、需求說明書

請另見文件-附件一

# 附件二、線框稿示意圖

請另見文件-附件二

# 附件三、軟硬體、技術規格及資安需求

1. 軟硬體環境之需求：

本專案在正式環境中所使用的硬體設備，將請得標廠商建議適用之雲端主機環境運行於本會私有雲，請得標廠商須以JAVA或.NET的執行環境、版本控管，並進行持續整合持續部署的機制作為軟硬體的環境建議。其運算資源及系統架構(如：作業系統種類、網站系統平台等)規劃需符合本會建置之私有雲使用規範為原則並撰寫於企劃書中，由本會另案租用相關運算資源以因應。本專案所需要之開發環境及測試環境由得標廠商協助建置。得標廠商準備之測試環境，應盡可能模擬正式環境情境，驗證功能完成且系統效能已達本專案之要求後，再移置至正式環境中。本專案系統使用之硬體及軟體將依得標廠商建議另案採購。

1. 使用者端
2. 硬體需求：

* CPU: 4 cores
* RAM: 8GB 以上

1. 軟體需求：

|  |  |
| --- | --- |
| 軟體 | 版本 |
| Microsoft Windows | 10 and above |
| Microsoft Edge   (Chromium) | All |
| Google Chrome | 75 and above |
| Mozilla Firefox | 60 and above |
| Safari | 12 and above |

1. 技術規格需求：
2. 本系統字元編碼一律採用 UTF-8。
3. 主要程式語言需使用物件導向式語言，如.NET C#或Java。
4. 程式前端可使用HTML5, CSS3, SCSS, TypeScript建構。
5. 須以 ORM 框架進行資料操作，除非必要，不使用 Stored procedure。
6. 如使用第三方程式套件，須提出合法使用之授權證明，並保障可運用於系統後續擴充之權益。
7. 如使用流程引擎，必須依循 BPMN 標準。
8. 以 Git作為版本控管機制，存放於本會 GitHub 儲存庫。
9. 資料庫建議採用SQL Server
10. 程式功能須以Restful API 等型態提供，並須有驗證、授權檢查機制。
11. 系統需支援微服務架構。
12. 能支援持續整合流程（Continuous Integration）與持續部署及自動化測試。
13. 主機須採用三層式網站資訊安全架構建置，外部資料僅可透過DMZ區主機導入，不得直接存取內網主機。
14. DMZ區主機與內網AP主機須使用特定埠(Port)連結，不得與內網DB主機直接連結。
15. 內外部使用者須可使用瀏覽器透過https(443 Port)直接使用本系統，無須透過VPN，其通訊傳輸須加密。
16. 行動裝置支援需求：本網站部分功能須響應式設計(Responsive Web Design)，以符合手機、平板等不同裝置使用者需求，需可於IOS(各版本)、Android(各版本)各不同系統清楚瀏覽、使用與體驗。
17. 分析報表需求：
    * + - 建議採用工具Tableau (online)並可用網頁崁入或API提供資料
        - 需要建置報表專用資料市集(Data Mart)與ETL的規劃
        - 請得標廠商規劃資料備份、索引調教及過期資料刪除、報表儲存空間
18. UIUX需求：

UX

* + 運用各種研究方法去了解使用者想法與需求（實驗、問卷、使用者訪談等）
  + 根據需求進行『User flow』、『Site Map』、『wireframe』、『Prototype』規劃
  + 透過『易用性測試』確認與評估產品是否符合使用者需求
  + 承上述，調整最終版並撰寫『功能規格書』
  + 交付上述文件資訊及功能規格書給UI設計師進行設計

UI

* + 配合甲方所擬定之設計規範（Design Guideline）
  + 繪製UI Design 並交由甲方審查
  + 繪製跨平台、跨裝置介面的操作一致性與易用性
  + 配合與PM、RD 的開發溝通與解決開發問題

1. 資安需求

投標廠商須就本專案建置系統所涉及有關安全部份，包含使用者身份認證、系統介接、網路資料安全等，提出規劃，並符合以下基本系統安全需求：

1. 系統管理功能須有使用權限之管制(權限控管、密碼強度依AD帳號管理辦法)，以識別使用者身分，決定使用者對資料及系統之使用權限，防止非合法授權人進入使用，即須有安全防護措施。每一獨立之系統頁面均須確保使用者具有相對之權限，以避免駭客以URL跳過登入之程序，直接進入系統之中。
2. 權限應區分應用程式使用者或一般使用者使用，應避免應用程式使用最高權限帳號啟用程式，如root、administrator 等帳號。
3. 一般使用者之帳號需以本會 Active Directory(AD) 進行登入驗證。
4. 密碼不可以明碼方式於任何地方顯示。
5. 帳號密碼等敏感性資料需使用加密傳輸（如：SSL）。
6. 密碼可配合本會資訊安全政策，隨時進行變更。
7. 需記錄使用者登入成功、失敗之歷程，並可於本系統管理後台查詢。
8. 網址URL上不可採明碼方式透漏使用者任何資訊。
9. 登入畫面須有驗證欄位(CAPTCHA)，防止惡意程式、機器人暴力破解。
10. 隱私資料必須加密，加密須採DES like 或AES like，128bit（以上）長度的key。
11. 廠商針對所開發的Web應用程式，應參考最新的OWASP (Open Web Application Security Project ) Top 10之常見弱點，廠商於交付開發程式時應提出足夠的佐證OWASP Top 10的弱點都已被排除，廠商將採用弱點掃描工具進行系統檢測，並於弱點掃描報告提出後，廠商需要依循問題內容進行軟體修改。廠商應針對系統安全的規格，包含但不限於：存取控制的機制(Access Controls)、密碼強度、重要或敏感性資料的保護、資料交換加密 (https， sftp)等提出說明。廠商未達成安全需求事項或未通過安全測試時，甲方將拒絕驗收，並要求限期改善。
12. 開發前、中、後應注意避免存在已知之安全漏洞，並進行安全檢測，如木馬程式檢測木馬、後門、間諜程式檢測、資料庫隱碼檢測及相關之安全測試，如發現有安全漏洞或後門程式，則須依本會資安規定，依問題等級A級所規範之時限內，立即進行補強。
13. 敏感資訊妥善處理，應用程式的安裝腳本不可留在系統中，帳號、廠商買主聯絡方法等敏感資料，不可被外部搜尋引擎取得或曝光。
14. 檢查使用者輸入內容與程式撰寫應避免SQL Injection 和XSS（Cross Site Scripting）攻擊手法，除了使用者輸入的資料以外，包含cookie和網址參數都要妥善處理。因此在任何使用者可以傳遞字元的地方，都要設下檢查機制，避免輸入<、>、%xx 等字串
15. 檢查上傳內容，避免上傳內容與檔名遭修改，造成對網站有危害的腳本程式被執行。
16. 前、後端都要檢查使用者輸入，避免網頁遭存回自己電腦，或透過JavaScript 語法修改DOM（Document Object Model），進而移除檢查機制。
17. 防止惡意人士對網站進行阻斷服務攻擊（Denial of Service, DoS）或分散式阻斷服務攻擊（Distributed Denial of Service, DDoS），在遭受攻擊時，系統也能夠正常運作。
18. 妥善處理錯誤訊息，避免當腳本語法或資料庫錯誤時，直接讓錯誤碼及相關資訊暴露在瀏覽器。資料庫檔案存取需具備管制功能，識別使用者對資料之使用權限，以防止非法授權進入系統存取資料。
19. 系統驗收前須執行滲透測試、弱點掃描及原始碼掃描，並提具資訊安全檢測報告。系統建置廠商需依據檢測報告，進行修補、改善處理，直到複測通過。此階段測試應委由公正「第三方專業測試廠商」代為執行，並交付相關報告。
20. 系統的維護作業，涵蓋新安全漏洞影響的預防與修補，並提供新增程式碼問題的修補，而非僅還原網站內容，造成系統漏洞一再被攻擊。
21. 錯誤控制：所有網頁均需提供Error Handling 機制，網頁原始碼不可顯示資料庫訊息，如主機名稱、資料表結構等資訊。
22. 提供完整登入稽核記錄及事件通知功能，其內容至少需包含何人、何地(Client IP)、何時、及發生事件等資訊。另包含陌生設備登入檢核通知功能。
23. 針對系統異常提供 E-mail 警訊功能，可讓管理者即時發現並立刻處理。
24. 使用者帳號等基本資料，如為機敏性資料需加密後儲存資料庫中。
25. 上述各項需求，廠商如建議更佳作法，經本會書面同意採用者，得取代原條文之要求。
26. 本系統開發各階段流程須遵循本會ISMS及相關法規要求。另要求廠商系統原始程式碼須通過本會源碼檢測工具檢測。

# 

# 附件四 、系統移轉需求

1. 介接測試

本專案開發之系統將介接營運管理相關之應用系統，並於各開發試階段進行該階段之系統介接測試，並於測試報告中說明測試項目及結果。

1. 系統移轉

本專案系統移轉規劃，以【新系統成功上線】與【既有服務不中斷】為最高指導，於系統建置中後期，由甲廠商共識討論，達成以下主要工作目標:

1. 提供移轉執行順序與時程。
2. 擬定系統服務移轉計畫，含硬體安裝設定計畫、軟體安裝設定計畫、資料移轉計畫、移轉測試計畫、服務切換計畫。

# 附件五 、建議書大綱

投標廠商交付之服務建議書章節大綱如下：

1. 廠商經驗與能力
2. 廠商簡介（內部組織人力、設施）
3. 近三年營運狀況簡介（營業額、服務範圍與能力）
4. 承接類似專案經驗實績與客戶滿意度（附件檢附證明文件）
5. 專案建置規劃方案
6. 專案概述
7. 整體系統架構及解決方案、教育訓練與技轉規劃說明
8. 營運能力優勢及服務水準
9. 優規

優於本規格書之項目，請自行製表說明。如有超出本案預算之額外金額，請一併列出。

| 項次 | 需求書優規需求 | 廠商優規內容大要 | 建議書頁次 |
| --- | --- | --- | --- |
|  |  |  |  |

1. 專案組織
2. 專案組織與人力配置：  
   本專案主持人、專案經理、工作人員及組織架構
3. 人力資源：  
   人力之質、量、資歷與證照
4. 分工與職掌
5. 專案管理工作說明
6. 專案工作時程規劃與完成期限
7. 專案提供之各項服務項目內容
8. 專業顧問之服務範圍、項目內容及相關文件
9. 交付項目及相關文件：  
   各項交付文件預計格式內容說明
10. 專案建置成本及範圍將依下列項目執行，請於規劃時列入考慮，並具據以提交建議書：
11. 專案建置成本包含專案實施、規劃、設計、測試及驗收相關文件
12. 專案上線前之技術移轉及教育訓練說明
13. 專案系統測試方案及驗收規劃，內容應包括:
14. 系統壓力測試
15. 系統資通安全測試等之測試方法
16. SIT/UAT使用者測試
17. 進行災難發生或硬體更換時，負責軟體之移置、回存、調整，或重新安裝（含作業系統、相關軟體元件及應用程式）之事件演練。
18. 系統效能測試部份應預估本系統正式作業時應有之作業效率、系統反應時間上限值等，並說明影響系統整體效能之因素及上述因素與系統反應時間彼此間關係之相關數據，說明驗證方式。
19. 對於上述相關將要求說明其測試方法，並擬定合理之商業標準並預估可達到之系統效能或相關數據，並說明影響上述測試效能之因素，及說明驗證方式。
20. 保固維護計畫及顧客服務：  
    內容應包括系統之維護保固工作團隊小組組織架構、人力分配及服務內容。提供維運手冊及教育訓練，說明系統平日檢查與發生異常時檢查及復原等流程。系統備份/備援計劃說明，須依照本會規定之備份/備援規範，訂定回復機制。
21. 教育訓練及技術移轉輔導計劃：  
    提供教育訓練計劃內容說明，包含各工作階段訓練執行內容及技術移轉輔導項目。應包含提供本案資訊系統委由廠商進行應用程式開發的客製化原始碼與第三方開放之原始碼。提供系統架構/環境，應用系統程式模組、後續系統維護、基礎建設、資訊安全團隊等相關範圍之說明。
22. 專案管理方法：  
    描述執行本專案時之作業流程管控、資源管控、需求變更管理、文件管理、風險管理、溝通管理、品質管理等方法。
23. 需本會配合事項
24. 成本分析與報價單明細
25. 專案總價及計價方式：須包括本專案期程內之報價總額(含應用程式開發、軟硬體規格報價)，並拆列各項目之單價。軟硬體設備將另案招標。
26. 其他相關費用及計價方式：若有其他費用，須一併列出並詳述計價方式。(包含視覺化工具、資料庫、應用程式軟體、其他配合本專案應用程式之專案管理工具、統計分析報表、第三方應用軟體導入、工具軟體版本升級、維護管理機制、版權費用等。）
27. 附件
28. 廠商經驗實績佐證文件
29. 專案小組成員履歷（學經歷相關證明、專案人員證照）
30. 其他附錄