

## 需求說明書

- 一、採購案名：分散式數據共享機制建置案
- 二、預算金額：新臺幣 20,000,000 元(含稅)
- 三、採購目的

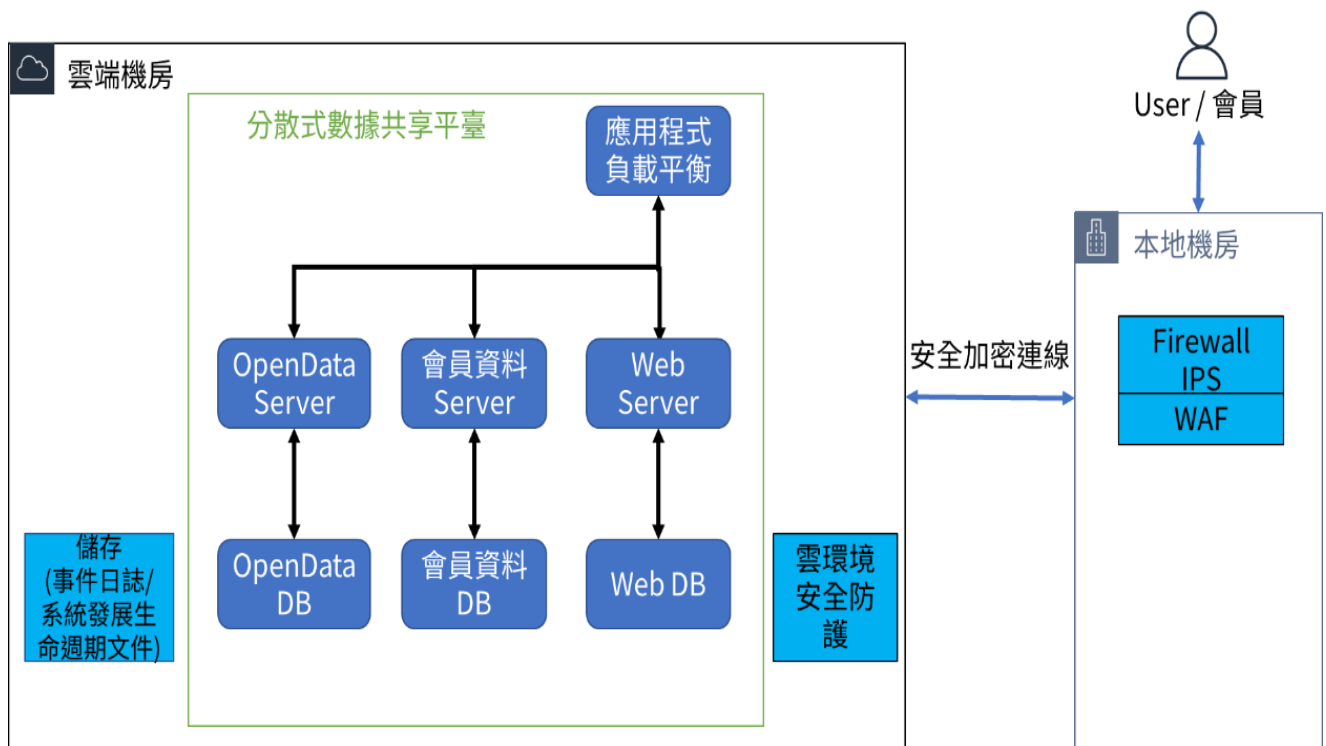
為執行政府補助計畫，建立具可信之數據交換機制，促進數據應用，本中心擬規劃建置「分散式數據共享機制」(以下簡稱本建置案)可讓公眾與產業信賴的數據交換或共享的平臺，推廣創新數據應用加值服務，透過平臺方式，有效媒合數據供需雙方，進一步強化數據使用效能。

本建置案目標為提供參與會員登錄、數據發布、隱私強化推廣、活動訊息、案例分享、開放資料等連結使用。

### 四、需求說明

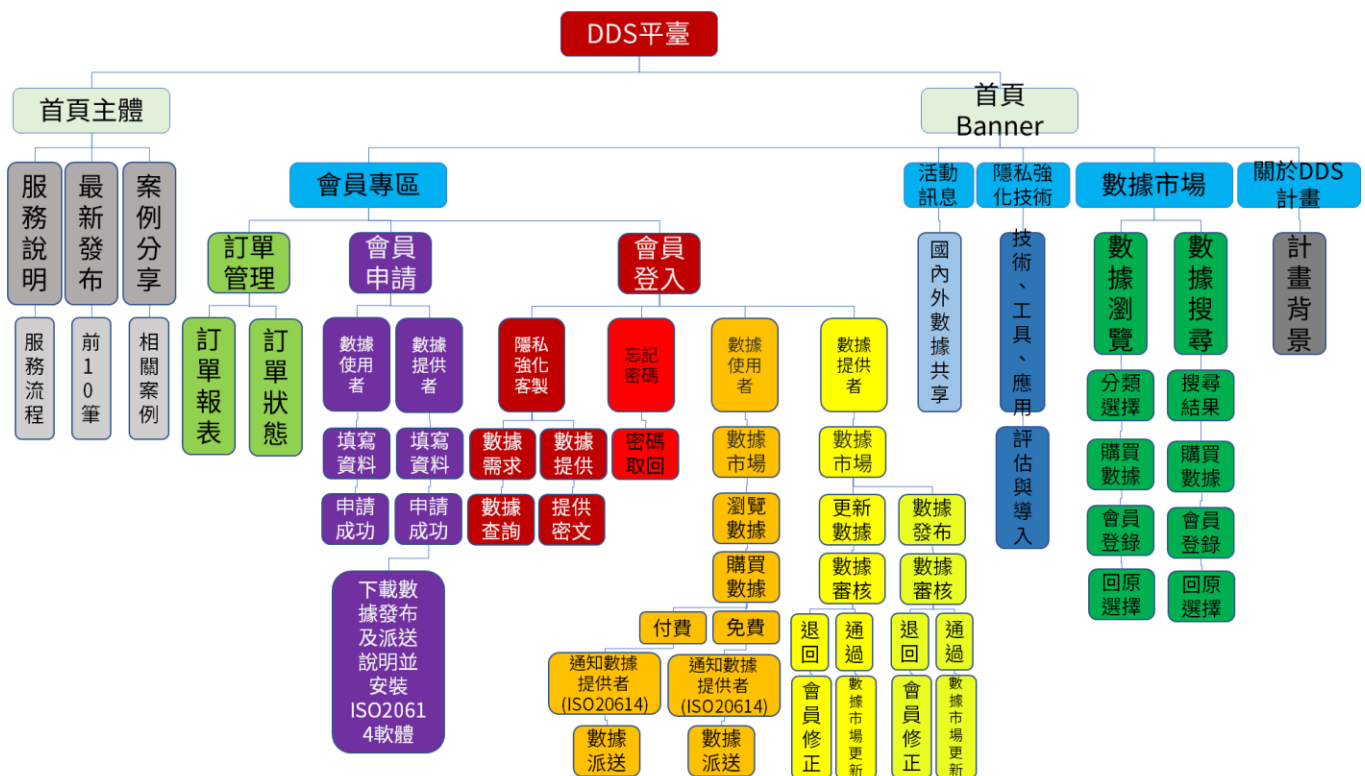
需求說明為本專案需求之基本規格建議，廠商在本建置案預算內，可另行於建議書中提供其認定之最適化建議或替代規劃建議，並考量未來整體發展方向及架構之擴充性，包含但不限於所列之項目。

#### (一) 系統架構說明：



圖表 1 - 系統架構圖

## 需求說明書



圖表 2 - 網站平臺架構圖

## (二) 系統功能需求說明

## 1. 網站前台需求

- (1) 帳號管理：提供數據提供者與數據使用者進行會員申請，帳號採雙因子驗證、以及零信任（Zero Trust, ZT）架構，並進行數據提供者公司驗證，確保數據由公司授權提供。
- (2) 數據發布：提供管理員數據審核，以及會員數據搜尋瀏覽與購買，並顯示各筆發布數據的審核進度供會員查看。
- (3) 訂單管理：由本中心 Active Directory 帳戶進行訂單狀態與報表之訂單管理，經付款確認後以 ISO 20614 規範通知數據提供者，以電子郵件通知數據使用者數據下載連結。數據使用者付款方式可採線上信用卡或匯款。
- (4) 隱私強化：建立隱私強化客製專區，串接數據提供者與數據使用者。
- (5) 案例分享：提供本中心案例分享之內容登載與維護功能。
- (6) 客製服務：提供會員提出客製服務登記頁面，以及管理客製服務進度。
- (7) 開放資料：提供免費開放資料(Open Data)，方便數據使用者應用。
- (8) 活動訊息：提供本計畫活動訊息或國內外數據共享活動之內容登載與維護功能。

## 2. 網站後台管理需求

- (1) 功能權限管控：系統功能、表單均能依照個人或群組權限設定逐項功能，可設定編輯或查看之權限，設定功能亦可透過系統管理者透過後台完成功能權限設定。
- (2) 後台內容維護需有版本紀錄功能，並提供回覆歷史版本功能。

## 需求說明書

- (3) 網站內容瀏覽統計，可針對網站單元、網站內容、日期區間等進行網頁造訪次數的統計。
- (4) 帳號管理：
  - A. 包含帳號之申請、建立、修改、啟用、停用及刪除之程序，不使用身分證字號為帳號名稱。
  - B. 已逾期之臨時或緊急帳號刪除或禁用。
  - C. 每半年定期審核帳號之申請、建立、修改、啟用、停用及刪除。閒置帳號經本中心同意後禁用。
  - D. 採最小權限原則，僅允許使用者依據本中心授權存取。
  - E. 對於每一種允許之遠端存取類型，均先取得授權，建立使用限制、組態需求、連線需求及文件化。
  - F. 使用者之權限檢查作業於伺服器端完成。
  - G. 監控遠端存取後台之連線。遠端存取採用加密機制。遠端存取之來源為本中心已預先定義及管理之存取控制點。
- (5) 會員管理功能：
  - A. 註冊：允許管理員查看、編輯、刪除用戶資料，例如企業名稱、統編、電子郵件、聯繫方式等，並且能夠審核和管理註冊申請。
  - B. 權限：管理員可以授權或取消用戶訪問特定功能或頁面的權限，以及管理用戶的角色設置。
  - C. 監控：記錄用戶的活動，例如登錄、註冊、數據傳輸、交易等，並提供報告和分析。
- (6) 交易管理功能：
  - A. 訂單：管理員可以檢視和處理訂單，例如更新訂單狀態、發送通知、查看付款記錄等。
  - B. 交易報告：提供交易報告和分析，例如總交易額、最受歡迎的交易類型、付款方式分析等。
- 3. 網站環境及擴充需求
  - (1) 擴充需求：需可在服務水準內完成擴充需求。
  - (2) 本建置案系統建置得使用虛擬伺服器架構，得標廠商須規劃本建置案系統架構及所需相關功能，負責完成整體系統與資料庫等之安裝建置與設定，並確保後續系統運作之正常。
- 4. 其他相關需求
  - (1) 須依數位發展部相關規範建置與維護(相關規定請參考行政院數位發展部「政府網站營運交流平台」，網址：<https://www.webguide.nat.gov.tw/>)，以及行政院數位發展部無障礙網頁規範製作無障礙網頁與申請標章(相關規定請參考行政院數位發展部「無障礙網路空間服務網」，網址：<https://accessibility.moda.gov.tw/>)之最新規範。
  - (2) 網站檢核分數需達到 70 分以上。
  - (3) 網站須符合無障礙網頁 AAA 級以上規範設計，並於配合本中心取得無障礙認證標章。
  - (4) 配合行政院「網際網路通訊協定升級推動方案」相關規定辦理資訊系統/網站 IPv6 升級(相關規定及檢測請參考網站 <https://www.gsnv6.tw/>)。

## 需求說明書

- (5) 全網站使用 https 加密連線(TLS1.2 以上版本，並提供 <https://www.ssllabs.com/ssltest/> 檢測佐證)。
  - (6) 網站可支援跨瀏覽器(支援 Chrome、edge、Safari、Firefox 等)。
  - (7) 頁面設計：提供單一網頁之整體之設計介面，包含選擇使用之樣板、選擇樣板各區使用之區塊及排版配置。另可依使用者社群屬性設計網頁，並提供多種版面之替換，惟版面之替換應考量整體網站風格一致性。
  - (8) 支援響應式網頁設計(Responsive Web Design, RWD)。
  - (9) 頁面設計：得標廠商須就本建置案之入口網站 layout 提供至少三個版型設計供本計畫補助機關選擇，並於第 1 期履約交付設計初稿，後續須配合補助機關意見修改並經本中心確認後執行。
  - (10) 平臺具備發生嚴重錯誤時之通知機制；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。
  - (11) 本建置案履約期限屆至時，由本中心提供地端伺服器設備，由廠商協助平臺網站保存事宜。
5. 安全管控需求
- (1) 除雙方另有約定外，得標廠商及其執行本建置案之人員應簽具本中心要求之保密文件並依約遵守保密規定。
  - (2) 得標廠商對本中心之業務機密負完全保密之責，且對補助機關之業務機密亦負完全保密之責。保密義務不因期限屆滿、解除或其他原因而終止後，得標廠商及其工作人員仍負有保密責任。
  - (3) 得標廠商及其工作人員因履行本建置案而取得之本中心業務資料，未經本中心同意，不得揭露與本建置案履行無關之第三人，如工作人員包含分包廠商(含個人)，應依約提供本中心審查。
  - (4) 得標廠商處理本標案相關之個人資料應遵守「個人資料保護法」之規定。
  - (5) 因應「個人資料保護法」及其施行細則之施行，本建置案如涉及個人資料之蒐集、處理及利用，應注意下列事項及相關法令：
    - A. 個人資料之蒐集或電腦處理，應經當事人書面同意、執掌必要範圍內、對當事人權益無侵害之虞，且符特定目的，始得為之（個資法修正施行後，應加上告知程序）。個資利用時，應與法定職務必要範圍內為之，並與特定目的相符。
    - B. 加強個人資料存取加解密及去識別化等防護功能，以及新增、修改、查詢、列印等必要 log 之記錄(且評估時應注意資料成長量及保存期限之規劃)。
  - (6) 得標廠商為執行本建置案所使用之軟體及各種文件不得抄襲、改作或任何侵害他人智慧財產權，若須引用，應加註出處。
  - (7) 得標廠商履行契約交付及使用之軟體，均須為合法軟體，不得違反著作權法、專利法及智慧財產權等相關規定。
  - (8) 得標廠商履行本建置案交付之程式碼與源碼檢測報告，應可在發生資安事故時再次進行源碼檢測，包含但不限於所繳交之版本，必須保證不含惡意程式(包含但不限於病毒、蠕蟲、特洛伊木馬、間諜軟體等)，隱密通道(covert channel) 或其它足以造成系統異常運作之措施。如發生資安事故時，本中心得將原始碼送交驗證單位進行檢驗，所需費用由得標廠商負擔，且須就本中心損失負賠償責任。



## 需求說明書

- (9) 如須於本中心網路環境下進行軟體開發、測試本建置案相關系統，得標廠商應依本中心作業規定辦理，同時以本中心正常上班時間內使用為原則，如須逾時使用，得標廠商應另行提出申請。
- (10) 因本建置案導致之資通安全事件，得標廠商應配合本中心要求辦理緊急應變及災難回復作業相關事宜。

### 6. 專案管理需求

- (1) 廠商須於第 1 期履約期限內提出工作計畫書，其內容包括對本計畫之執行敘述、專案團隊組織、人力、分工、職掌、計畫工作項目及時程、專案管理與監控、確認與驗收等。
- (2) 專案執行管控：計畫執行期間得標廠商須配合出席本中心所召開之專案工作會議，由得標廠商對專案進度進行工作報告，同時對專案工作所要求之期程、品質、風險，如有發生管控異常時，得標廠商應提具建議方案，並於會議中與本中心進行溝通協調，同時如本計畫補助機關數位發展部數位產業署欲針對專案細節進行了解與討論，得標廠商需配合本中心派員出席。

### (三) 軟/硬體設備需求與規格

#### 1. 雲端服務資源租賃需求：

- (1) 中央處理器需為 Intel Xeon 處理器需具備可達 3.4 GHz。
- (2) 單一主機需可擴充規格至 96 vCPU 和 192 GiB 記憶體。
- (3) 伺服器的聯網頻寬，最高可達 25 Gbps。
- (4) 伺服器掛接的儲存存取頻寬，最高可達 19 Gbps 頻寬。
- (5) 作業系統可支援：Ubuntu、Windows Server、Red Hat Enterprise Linux、SUSE Linux Enterprise Server 等。
- (6) 資料庫可支援：MySQL、MariaDB、Oracle、SQL Server、PostgreSQL 等。
- (7) 系統備援：原服務中斷時，於服務水準時間內，由備援設備或其他方式取代並提供服務。
- (8) 雲端分析服務：提供存取分析服務數據應用，並可隨時擴充使用容量。
- (9) 負載平衡服務：具備 HTTP(S) 負載平衡功能來平衡各項工作負載，動態擴展及縮減能力，因應流量調整增(減)配置虛擬主機。
- (10) 虛擬專用網路：提供 VPN 連接支援地端和雲端環境之間的安全連線，提供 VPN 通道支援資料在地端和雲端環境之間往返傳送的加密連結，以及支援網際網路金鑰交換版本 2(IKEv2)。
- (11) 漏洞管理服務：掃描雲端並評估是否存在已知漏洞，自動化發現和持續掃描漏洞問題，集中管理、設定和檢視所有的問題清單，並提供問題清單的風險評分。
- (12) 防毒服務：提供抵禦惡意軟體的即時防護功能，以及自動威脅防護政策建議，為 Cloud Marketplace 服務，可於雲端平臺上正常運行。
- (13) DDoS 攻擊防禦：於發生攻擊時提供自動保護，以維持服務運作，提供保護所有使用的雲資源。
- (14) 監控告警服務：提供雲端環境相關發掘錯誤設定和安全漏洞檢測報表，於事件發生時，提供稽核追蹤紀錄，並提供進階持續性威脅攻擊防禦措施。
- (15) 雲端服務須通過國際資安標準驗證 ISO 27001。
- (16) 雲端需求數量如下：

## 需求說明書

- A. 平臺 AP：1 台，單台虛擬處理器須提供 4 個(含)以上，記憶體容量須提供 16 GiB(含)以上，儲存容量須提供 300GB SSD (含)以上，網路介面速度須提供最高可達 10 Gbps。
  - B. 平臺 DB：2 台，單台虛擬處理器須提供 4 個(含)以上，記憶體容量須提供 16 GiB(含)以上，儲存容量須提供 300GB SSD (含)以上，網路介面速度須提供最高可達 10 Gbps。
  - C. 虛擬儲存池：儲存空間須提供 1TB 的可用空間(含)以上，未來可依需求擴展，提供 Web 服務介面，用於管理操作。
  - D. 虛擬資源：決標 日起至 112 年 12 月 31 日提供 12 台，113 年 1 月 1 日起提供 24 台，單台虛擬處理器須提供 4 個(含)以上，記憶體容量須提供 8 GiB(含)以上，儲存容量須提供 100GB SSD (含)以上，網路介面速度須提供最高可達 10 Gbps。
- (17) 系統發展生命週期
- A. 針對本建置案之資安風險評估，包含可能之資通系統機密性、完整性、可用性風險，及採取之對應控制措施。
  - B. 根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。
  - C. 將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。
  - D. 針對安全需求實作必要控制措施。
  - E. 軟體常見漏洞及實作必要控制措施。
  - F. 於部署環境中針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。
  - G. 系統不使用預設密碼。
  - H. 原始程式庫新增、修改、修改存取控制措施並留有稽核日誌記錄存取行為，於系統發展生命週期之維運階段，執行版本控制與變更管理。
  - I. 開發、測試及正式作業環境應為區隔。
  - J. 儲存與管理系統發展生命週期之相關文件，以書面或電子化形式保存，並被納入管理程序。
  - K. 系統之漏洞修復測試有效性及潛在影響，兩週內提供解決方案與說明報告，並於一個月或議定期限內修補完成。
  - L. 每週定期確認系統相關漏洞修復之狀態。
  - M. 發現系統有被入侵跡象時，通報本中心系統相關人員。
  - N. 監控資通系統，以偵測攻擊與未授權之連線，並識別系統之未授權使用。
  - O. 使用防毒軟體或完整性驗證工具，以偵測未授權變更特定軟體及資訊。
  - P. 使用者輸入資料合法性檢查置放於應用系統伺服器端。
  - Q. 發現違反完整性時，系統實施本中心指定之安全保護措施。因應網頁置換攻擊。
  - R. 廠商依『國家資通安全研究院』發布的漏洞警訊公告，無條件優先進行修補，必要時需配合修改所開發之程式及更新系統工具版本。
2. 地端硬體防火牆設備全新品租賃一台
- (1) 提供 Site-to-Site VPN 功能，並可利用 IPSec 以及 SSL 協定進行 Site-to-Site VPN 連線。

## 需求說明書

- (2) 支援 IPv4 與 IPv6 網路路由功能。
  - (3) 提供使用者認證機制，包括內建資料庫及外部 RADIUS、LDAP、Active Directory、eDirectory、TACACS+ 等認證伺服器，支援 Active Directory 和 eDirectory 單一簽入(Single Sign-On)機制。
  - (4) 防火牆處理效能最大須達 38,000Mbps(含)以上，同時連線數最大須達 12,000,000 條(含)以上。
  - (5) 切換威脅防護模式(Threat Protection)處理效能最大須達 2000Mbps(含)以上。
  - (6) 切換入侵防禦機制模式處理效能最大須達 9500Mbps(含)以上。
  - (7) 須提供雙因子驗證(One Time Password)機制，並可在防火牆網頁管理頁面、IPSec 和 SSL VPN 啟用此驗證機制，強化登入安全強度。
  - (8) 防火牆特徵資料庫(Signature Database)需能透過網路更新，並免費提供特徵資料庫更新服務，得標廠商須提供原廠資料庫更新服務證明文件。
  - (9) 得標廠商得標後須提供原廠在台辦事處授權經銷暨連帶服務證明。
  - (10) 防火牆設備需可提供相關網路安全防禦機制服務：
    - A. 提供偵測殭屍網路(Botnet)及命令與控制(C&C)伺服器和惡意網站。
    - B. 須提供入侵防護功能，並具備針對不同作業系統平台預先設定好的類別，如 Windows、Linux、UNIX、Mac、BSD 和 Solaris 等，方便管理者設定相關防護條件。
    - C. 可針對任何網路或使用者自訂不同的 IPS 政策、且特徵碼可自動更新並支援自訂 IPS 特徵檔。
3. 地端硬體網頁應用防火牆設備全新品租賃一台
- (1) 提供 Site-to-Site VPN 功能，並可利用 IPSec 以及 SSL 協定進行 Site-to-Site VPN 連線。
  - (2) 支援 IPv4 與 IPv6 網路路由功能。
  - (3) 提供使用者認證機制，包括內建資料庫及外部 RADIUS、LDAP、Active Directory、eDirectory、TACACS+ 等認證伺服器，支援 Active Directory 和 eDirectory 單一簽入(Single Sign-On)機制。
  - (4) 防火牆處理效能最大須達 38,000Mbps(含)以上，同時連線數最大須達 12,000,000 條(含)以上。
  - (5) 切換威脅防護模式(Threat Protection)處理效能最大須達 2000Mbps(含)以上。
  - (6) 切換入侵防禦機制模式處理效能最大須達 9500Mbps(含)以上。
  - (7) 須提供雙因子驗證(One Time Password)機制，並可在防火牆網頁管理頁面、IPSec 和 SSL VPN 啟用此驗證機制，強化登入安全強度。
  - (8) 網頁應用防火牆特徵資料庫(Signature Database)需能透過網路更新，並免費提供特徵資料庫更新服務，得標廠商須提供原廠資料庫更新服務證明文件。
  - (9) 得標廠商得標後須提供原廠在台辦事處授權經銷暨連帶服務證明。
  - (10) 網頁應用防火牆設備需可提供相關網路安全服務：
    - A. 提供偵測殭屍網路(Botnet)及命令與控制(C&C)伺服器和惡意網站。
    - B. 須提供入侵防護功能，並具備針對不同作業系統平台預先設定好的類別，如 Windows、Linux、UNIX、Mac、BSD 和 Solaris 等，方便管理者



## 需求說明書

設定相關防護條件。

- C. 可針對任何網路或使用者自訂不同的 IPS 政策、且特徵碼可自動更新並支援自訂 IPS 特徵檔。
  - D. 須提供 HTTP、HTTPS、FTP、等協定進行的病毒、網頁惡意軟體、木馬程式和間諜程式偵測功能，並可自動更新防毒特徵碼。
  - E. 須具備 Pharming Protection 和 JavaScript 模擬功能，有效阻擋進階網頁威脅
  - F. 須提供即時雲端查詢可取得最新的威脅情報。
  - G. 須提供針對使用者或群組網頁瀏覽配額時間和存取時間的管控。
  - H. 提供網頁政策覆蓋功能，讓管理者可以暫時瀏覽被阻擋的網站或類別，以利除錯和觀察有問題的網站。
  - I. 須可支援 92 個(含)以上 URL 網站類別，且管理者可以依據 Mime 類型、副檔名、ActiveX、Applet 和 Cookie 等檔案類型進行過濾。
4. 本建置案所建置系統中所使用之軟體、資料庫、API，均由得標廠商提供（如使用第三方授權軟體或工具應於履約時一併交付使用授權文件），同時須規劃並保留未來擴充能力，廠商需就擴充能力進一步說明產品之特色。

### （四）系統、軟/硬體設備試運轉及測試需求

- 1. 雲端系統之測試及正式作業環境應作區隔，透過帳戶層級的區隔，將測試環境與正式環境的工作負載及網路環境隔離。
- 2. 廠商應自備壓力測試工具，並事前提請本中心審查同意後，以該工具執行壓力測試。壓力測試結果，應能呈現本建置案開發之網站的系統處理能力，包括每分鐘最大可承受之使用者數。
- 3. 本建置案須於上線前於正式環境進行壓力測試，分別以電腦模擬同時間內 200 個以上的使用者連線至本建置案網站系統，以量測首頁圖文完全開啟所需之時間，90%使用者應小於或等於 3 秒，並提供「網站系統壓力測試報告」。

### （五）教育訓練需求

得標廠商須就本建置案之工作事項提供詳細之教育訓練及技術移轉，相關細節說明必須於專案工作計畫書中說明並經本中心確認後執行，其內容應包含如下：

- 1. 系統建置、管理、操作教育訓練相關文件與執行方式、執行時數。
- 2. 為確保技術移轉及訓練之落實，需提供本建置案技術移轉訓練計畫，訓練時數不得低於 16 小時，本中心將視訓練執行情形得調整執行方式，以達成本中心自行維運之目標。

### （六）系統、軟/硬體維護需求

系統(網站)維護方式：以遠端維護，並限制來源 IP，透過 SSL VPN+多因子身分驗證。

### （七）系統資通安全需求

- 1. 廠商配合本中心於「資通安全責任等級分級辦法」之分級及控制措施，配合修正系統防護，以符合對應等級之規範。
- 2. 廠商配合本中心於 ISMS、內(外)部稽核、營運持續演練、監控管理及安全性檢測等各項工作。
- 3. 執行本建置案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊



## 需求說明書

產品。

4. 廠商提供之雲端服務需確保不得設置存放於中國大陸地區（含香港與澳門地區）及可能曝露高風險區域。
5. 每半年執行主機及網站安全弱點檢測，檢測符合最新版 OWASP TOP10 的項目。每年執行滲透測試與資通安全健檢（包含網路架構檢視，防火牆與目錄伺服器設定檢視，惡意活動檢視），並提供解決方案與說明報告。
6. 事件日誌
  - (1) 作業系統日誌(OS event log)、網站日誌(Web log)、應用程式日誌(AP log)、登入日誌(Logon log)，訂定日誌之記錄時間週期及紀錄留存政策，並保留日誌至少六個月。
  - (2) 確保系統有記錄特定事件之功能，並決定應記錄之特定系統事件。如：身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及等。
  - (3) 記錄系統管理者帳號所執行之各項功能。如：帳號登出入、密碼變更、存取權限異動等。
  - (4) 每週定期審查本中心所保留系統產生之日誌。
  - (5) 系統產生之日誌包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式的一致性，並依資通安全政策及法規要求納入其他相關資訊。
  - (6) 依據日誌儲存需求，配置所需之儲存容量。（配置最少 6 個月之儲存容量）
  - (7) 於日誌處理失效時，採取適當之行動。（如：儲存容量空間不足，選擇進行封存，不要覆寫日誌資料）
  - (8) 使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。
  - (9) 每週系統內部時鐘定期與基準時間源進行同步。
  - (10) 對日誌之存取管理，僅限於有權限之使用者。
  - (11) 運用雜湊或其他適當方式之完整性確保機制。
7. 營運持續計畫
  - (1) 執行系統源碼與資料備份。
  - (2) 每季定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。
8. 識別與鑑別
  - (1) 系統具備唯一識別及鑑別本中心使用者功能，以雙因子驗證、以及零信任（Zero Trust, ZT）架構，禁止使用共用帳號。
  - (2) 使用預設密碼登入系統時，應於登入後要求立即變更。（例如透過系統機制要求使用者登入後立即變更密碼）
  - (3) 身分驗證相關資訊不以明文傳輸。
  - (4) 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用本中心自建之失敗驗證機制。
  - (5) 使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。（密碼不少於 12 碼，且由大小寫、數字及符號組成混合，且需在一定期間[1~90 天]內變更）
  - (6) 密碼變更時，至少不可以與前三次使用過之密碼相同。
  - (7) 對非內部使用者，可依本中心自行規範密碼設定強度、效期與密碼不重複次數。

## 需求說明書

- (8) 身分驗證機制防範自動化程式之登入或密碼更換嘗試。(應有 captcha 機制)
- (9) 密碼重設機制對使用者新身分確認後，發送一次性及具有時效性符記。
- (10) 系統應遮蔽鑑別過程中之資訊。(如:以\*取代真實輸入字元)
- (11) 系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。

## (八) 原始碼需求

1. 本建置案平臺程式原始碼及執行檔，須以電子郵件加密方式提供本中心承辦人員，以利本中心管控程式版本。
2. 本建置案所購置取得之軟體與原始碼，若有未非廠商自行開發之項目，需提供來源出處及授權等相關證明。(包括但不限於：開源專案名稱、出處資訊、原始著作權利聲明、免責聲明、開源授權條款標示與全文)

## 五、履約期限

- ☐ 應於○年○月○日以前完成。
- ☐ 應於決標之日起○日曆天/工作天完成。
- ☒ 其他：決標日起至 113 年 12 月 31 日。

## 六、履約期程及交付項目表(以下簡稱表 1)

項次	履約期限	交付項目	交付格式
1	決標後 10 日	1.1 保密同意書 1.2 保密切結書 1.3 啟動會議簡報 1.4 工作計畫書 1.5 網站版面設計初稿	除 1.1 及 1.2 交付紙本 1 式 1 份，其餘交付格式如下： <input checked="" type="checkbox"/> 紙本 1 式 2 份 <input checked="" type="checkbox"/> 電子檔 1 式 1 份
2	112 年 6 月 30 日	2.1 系統建置規劃書 2.2 系統規格說明書 2.3 系統功能說明書 2.4 系統上線計畫書 2.5 軟、硬體授權或新品證明文件 2.6 防火牆資料庫更新原廠授權證明	<input checked="" type="checkbox"/> 紙本 1 式 2 份 <input checked="" type="checkbox"/> 電子檔 1 式 1 份
3	112 年 7 月 31 日	3.1 交付原始碼及源碼檢測報告 3.2 系統弱點掃描暨修補報告 3.3 系統測試報告書	<input checked="" type="checkbox"/> 紙本 1 式 2 份 <input checked="" type="checkbox"/> 電子檔 1 式 1 份
4	112 年 8 月 31 日	4.1 系統、軟/硬操作手冊 4.2 教育訓練教材、簽到表	<input checked="" type="checkbox"/> 紙本 1 式 2 份 <input checked="" type="checkbox"/> 電子檔 1 式 1 份
5	113 年 01 月 31 日	112 年維護紀錄	<input checked="" type="checkbox"/> 紙本 1 式 2 份 <input checked="" type="checkbox"/> 電子檔 1 式 1 份

## 七、履約地點

- ☐ 本中心高雄本部(高雄市路竹區路科一路 3 號)
- ☐ 本中心新北辦公室(新北市板橋區遠東路 1 號 3 樓)
- ☒ 其他指定場所：依本中心指定地點。

## 需求說明書

### 八、驗收

#### (一) 數量及規格點收：

1. 廠商交付之採購標的須齊全（包含各原廠標準出貨時所附配件與使用手冊），應符合契約規定，無減少或減失價值或不適於通常或約定使用之瑕疵，且為全新未經拆封使用，並保留原製造廠商出貨時之完整包裝及貼封全新品（所有標的相關零配件及連接線亦同）。
2. 採購標的如廠商須先拆封測試者，須經本中心同意後才能進行拆封，拆封時亦須會同本中心人員。
3. 廠商交付採購標的後，經本中心初步數量、規格點收後，其中任何一項數量、規格不符或非新品，視同不合格。

#### (二) 系統測試：

1. 依「四、需求說明」中相關需求及確認後之需求內容進行測試，並產出相關測試報告。
2. 本建置案採購標的由廠商派員至本中心執行測試，均能正常執行且正常運作於相關軟硬體設備與系統，經功能測試合格後，本中心始認可廠商所提供之軟硬體設備。

#### (三) 其他

1. 本中心採購金額達新臺幣 150 萬元採購案，得標廠商各期履約交付，應於履約標的預定完成履約日前或完成履約當日，將完成履約日期以書面通知本中心辦理驗收。
2. 分期驗收方式：採書面文件配合系統功能或者以雙方約定之驗收方式進行。
3. 其他依本中心驗收規定辦理驗收。

### 九、付款條件

☐ 一次付清：廠商於完成表 1 項次○至項次○所有履約交付項目，並經本中心驗收合格，且無待解決事項後，本中心一次付清決標價金總額。

☒ 分期付款：

第一期：廠商於完成表 1 項次 1 及項次 2 履約交付項目，並經本中心驗收合格後，且無待解決事項後，撥付決標價金總額 50%。

第二期：廠商於完成表 1 項次 3 及項次 4 履約交付項目，並經本中心驗收合格後，且無待解決事項後，撥付決標價金總額 25%。

第三期：廠商於完成表 1 項次 5 履約交付項目，並經本中心驗收合格後，且無待解決事項後，撥付決標價金總額 25%。

☐ 其他：

### 十、保固及維護需求

#### (一) 保固需求：

☐ 自驗收合格之日起，得標廠商須提供保固○年。

☐ 自驗收合格次日起，得標廠商須提供保固○月/年。

## 需求說明書

☐自驗收合格之日起，得標廠商須提供系統○年、軟/硬體設備○年保固服務。

### (二)維護服務：

1. 維護期間：第一期驗收完成後至 113 年 12 月 31 日，本建置案採租賃方式委託得標廠商依據本需求書維護本機制。
2. 得標廠商提供本建置案維護期間內之軟硬體設備維護，以確保本建置案所採購之系統設備在維護期間內的可用性，每季乙次到場系統維護保養，並提供設備狀態分析，將定期維護之紀錄乙份留存本中心。
3. 本建置案維護期間內的系統設備維修之時間為星期一至星期五上午九點至下午五點，例假日不在此限。
  - (1) 本建置案維護期間內，得標廠商須提供電話及到場維修服務；
  - (2) 設備若發生異常，廠商須於 8 工作小時內回應，若無法線上將異常問題排除，廠商須於 16 工作小時內到場處理。
  - (3) 設備故障須於 24 工作小時內修復完畢。
  - (4) 設備故障之程度如無法現場維修必須攜回處理，或維修超過 24 工作小時(含)以上仍無法回復正常運作時，得標廠商應提供同等級之設備替代使用(是否屬同等級由本中心專案人員認定之)，並應於 30 日曆天內將原設備修復送回本中心。
4. 本建置案履約期限屆至時，廠商應通知本中心辦理設備回收事宜，如逾 7 日未通知本中心，則由本中心自行處理。

## 十一、資安需求

### (一)本建置案資通系統籌獲

1. ☐涉及本中心(或委託/補助機關)之核心資通系統(本款未勾選者，為非核心資通系統)
2. 本建置案資通系統之防護需求等級：  
☐高  
☒中  
☐普

### (二)資安法需求

依照資通安全管理法施行細則之要求，廠商須配合事項如下：

1. 得標廠商辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。
2. 得標廠商應配置充足且經適當之資格訓練，擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。
3. 本採購案不得轉包，得標廠商應依據契約書辦理。
4. 本建置案得標廠商☐不得分包；☒得分包
  - (1)得標廠商得分包項目如下:弱點掃描、滲透測試、資安健檢
  - (2)得標廠商應於分包前提交分包工作計畫書供本中審查。



## 需求說明書

5. 本採購案為■客製化資通系統開發，得標廠商應提供本建置案資通系統之下列安全性檢測證明：（本款未勾選者，不適用本條文）

■弱點掃描

■滲透測試

■源碼掃描

6. 得標廠商執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知本中心及採行補救措施。
7. 得標廠商應於委託關係終止或解除時，返還、移交、刪除或銷毀履行合約而持有之資料，並留存處理紀錄以供本中心查核。
8. 得標廠商應說明採取之其他資通安全相關維護措施。
9. 得標廠商應配合本中心以稽核或其他適當方式確認受託業務之執行情形。
10. 本採購案包含■客製化資通系統開發，廠商須配合下列事項：（本款未勾選者，不適用本條文）
- (1) 得標廠商所使用之開源工具，需提供工具取得來源(透明性)及開發者之相關證明文件(可追溯性)。
  - (2) 本採購案資通系統中涉及利用非得標廠商自行開發之系統或資源者，投標廠商應於服務建議書標示非自行開發之內容與其來源，並於得標後提供授權證明。
11. ☐本採購案涉及國家機密，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。（本款未勾選者，不適用本條文）

(三)其他資訊安全需求：廠商須提供前述系統發展生命週期管理服務。

## 十二、履約保證金

☐無。

■廠商於決標日起 14 日曆天內應繳納履約保證金，金額為合約金額 10%。

## 十三、保固保證金

■無。

☐廠商於驗收合格日起 14 日曆天內應繳納保固保證金，金額為合約金額 3%。

## 十四、投標廠商資格文件

■1. 廠商登記或設立證明。

■2. 廠商納稅證明。

■3. 廠商須具備雲端平臺建置、以及中級資通系統防護基準經驗，並提供相關實績證明文件佐證。

■4. 本建置案屬「具敏感性或國安(含資安)疑慮之業務範疇」之資訊服務採購，廠商不得為經濟部投資審議委員會公告之陸資資訊服務業者。

■5. 本中心全面適用 ISO 27001 規定，本中心資通作業委外採購案，廠商須提供辦理

## 需求說明書

受託業務之相關程序或環境通過資通安全管理制度第三方驗證之證明。

- 6. 本中心全面適用 ISO 27001 規定，本中心資通作業委外採購案，廠商須提供服務團隊成員中應包含具有資通安全專業人員至少一名並檢附證明文件。
- 7. 其他：「雲端服務提供者須具備雲端資安相關第三方認證資格」，例如 ISO/IEC 27017 雲服務資訊安全管理標準或 CSA STAR 雲端安全認證。

### 十五、聯絡方式

(一) 請購單位：江先生

電子信箱：Jay.Chiang@ttc.org.tw/連絡電話：(02)8953-5650

(二) 採購單位：陳先生

電子信箱：Eric.Chen@ttc.org.tw/連絡電話：(02)8953-5956

### 十六、企劃書(或服務建議書)製作規定

(一) 裝訂與數量：

1. 裝訂：請用 A4 規格雙面印刷，內容以中文直式橫書繕打，並併同目錄(含目次、頁次)裝訂成冊且各部分之章節號碼須前後統一，並標註頁數。
2. 數量：投標廠商須於投標期限內提送企劃書紙本 1 式 10 份及電子檔(USB 隨身碟或光碟片以 Microsoft 系列編輯軟體製作與 PDF 軟體製作) 1 式 2 份送達本中心指定收件處所。

(二) 一般要求：

1. 製作企劃書及契約簽訂前所費之成本，由投標廠商自行負擔，得標廠商之企劃書及簡報資料所佐附證明文件需清晰可讀，以上資料所有權歸本中心，並視為契約應履行部份。
2. 企劃書交付後，本中心得交付評選委員審核、工作小組成員初審及承辦人員承辦，不得交付其他人員參閱。
3. 企劃書及所有參考資料，評選後概不退還。
4. 如有未盡事宜，以本中心解釋為準。

(三) 企劃書應包括章節如下表項目所示：(須與評選項目、內容相符)

1. 專案簡介(專案名稱、專案目標)
2. 廠商規模及經驗實績(含資安人力等)
3. 專案團隊人力及技術能力(含資安專業能力)
4. 專案規劃內容(專案範圍、專案時程)。
5. 軟/硬體規格說明
6. 系統功能規劃
7. 廠商資安作為(須提供資安管理作業自我評估表，請參考附件 1 範例)
8. 教育訓練規劃
9. 廠商標價及標價組成內容(含資安作業經費，資安作業經費編列方式請參考附件 2)

## 需求說明書

10. 驗收規劃

11. 答標對照表(請參考附件 3)

(四) 評選標準：

評選項目	內容	配分
一、廠商規模及經驗實績	<ul style="list-style-type: none"> <li>● 廠商規模、背景、資安相關政策、認證(含資安認(驗)證)、獎項、人力資源(含資安人力)</li> <li>● 最近3年營運實績</li> <li>● 最近3年營運狀況</li> <li>● 履約實績</li> </ul>	15
二、專案團隊人力及技術能力	<ul style="list-style-type: none"> <li>● 專案組織(含資安)</li> <li>● 人力配置(含資安)</li> <li>● 團隊成員履約能力</li> </ul>	15
三、專案規劃內容	<ul style="list-style-type: none"> <li>● 系統建置規劃 (軟硬體規格、系統功能、教育訓練等)</li> <li>● 平臺持續性營運規劃</li> <li>● 服務品質管理規劃</li> </ul>	30
四、資安作為	<ul style="list-style-type: none"> <li>● 履約程序及環境之資安管理規劃及執行方式</li> <li>● 履約相關之資安事件通報、應變、處理之規劃機制</li> <li>● 資安作為自評情形</li> </ul>	10
五、廠商標價及標價組成內容	標價及標價組成內容合理性	20
六、簡報及答詢	<ul style="list-style-type: none"> <li>● 廠商簡報</li> <li>● 廠商答詢</li> </ul>	10
總分		100

## 需求說明書

附件 1

**(廠商名稱) 參與財團法人電信技術中心辦理 (標的名稱) 案之相關資安管理作業自我評估表 (範例)**

日期： 年 月 日

評估項目	辦理情形
<b>1. 管理面</b>	
1.1 辦理本建置案受託業務相關程序及環境之資通安全管理措施或通過第三方驗證	<input type="checkbox"/> 辦理本建置案受託業務之相關程序及環境已(將)通過_____認(驗)證並持續有效，驗證公司為_____ <input type="checkbox"/> 辦理本建置案受託業務之相關程序及環境已具備完善資安管理措施，詳_____文件(如未載明於既有文件內，請於備註欄內說明相關措施) <input type="checkbox"/> 本建置案受託業務之相關程序及環境未導入適當資安管理措施 備註：_____
1.2 本建置案之資安負責人、資安專責主管或其他資安人員之人力配置規劃	<input type="checkbox"/> 本建置案之資安負責人(專案主管)為_____ <input type="checkbox"/> 本建置案之資安人員為_____ <input type="checkbox"/> 本建置案未指派資安負責人、資安專責主管或其他資安人員 備註：_____
1.3 本建置案之資安風險評估，包含可能之資通系統機密性、完整性、可用性風險，及採取之對應控制措施	<input type="checkbox"/> 本建置案受託業務相關程序及環境之資安風險評估結果已(將)載明於_____文件，已(將)採取對應之控制措施詳_____文件(如未載明於既有文件內，請於備註欄內說明相關措施) <input type="checkbox"/> 未就本建置案進行資安風險評估 備註：_____
1.4 本建置案範圍內之資安事件通報應變程序，包含知悉資安事件發生或有發生之虞之相關通報時效規定、通報方式、資安事件調查、處理及改善流程	<input type="checkbox"/> 本建置案受託業務相關程序及環境之資安事件通報應變程序已(將)載明於_____文件(如未載明於既有文件內，請於備註欄內說明相關措施)，知悉資安事件或發現有事件發生之虞時，應於__小時內向甲方等相關利害關係人通報，通報對象包含_____ <input type="checkbox"/> 未就本建置案訂定相關資安事件通報及應變程序 備註：_____
1.5 由招標公告日起算，過去3年是否發生因管理議題肇因之重大資安事件	<input type="checkbox"/> 過去3年無發生因管理議題肇因之資安事件 <input type="checkbox"/> 是，共__次，事件發生主要根因為_____ 備註：_____



## 需求說明書

2. 技術面	
2.1 本建置案範圍內之資通系統，包含主要履約標的之資通系統及其他執行本建置案業務所需使用之業務、行政相關資通系統，辦理安全性檢測	<input type="checkbox"/> 本建置案範圍內之資通系統將規劃執行_____（如源碼掃描、弱點掃描、滲透測試），檢測項目及本建置案範圍為：_____ <input type="checkbox"/> 未就本建置案範圍內之資通系統規劃安全性檢測 備註：_____
2.2 辦理本建置案受託業務環境及設備導入之相關資通安全防護措施	<input type="checkbox"/> 本建置案受託業務之環境及設備已（將）導入（啟用）_____（如防毒軟體、防火牆、電子郵件過濾機制、入侵偵測及防禦機制等），導入項目及本建置案範圍為：_____ <input type="checkbox"/> 本建置案受託業務之環境及設備未導入相關資通安全防護措施 備註：_____
2.3 本建置案範圍內之資通系統及專案資料之存取控制等權限管理機制，如 PM、系統管理員、一般使用者帳號之權限分級原則及控管方式	<input type="checkbox"/> 本建置案範圍內之資通系統帳號或使用者權限分成__種等級，相關存取控制、權限管理機制說明如下：_____ <input type="checkbox"/> 未規劃本建置案範圍內之資通系統及專案資料相關存取控制及權限管理機制 備註：_____
3. 認知訓練面	
3.1 本建置案直接履約相關人員之資安教育訓練	<input type="checkbox"/> 本建置案直接履約相關人員之資安教育訓練包含__小時之資安通識教育訓練，對象包含_____；__小時之資安專業教育訓練，對象包含_____ <input type="checkbox"/> 未規劃相關資安教育訓練 備註：_____
3.2 本建置案團隊人員取得之資通安全專業證照	<input type="checkbox"/> 本建置案具資安證照之團隊成員有：__位 <input type="checkbox"/> 本建置案團隊人員未具備資通安全專業證照 備註：_____



## 需求說明書

## 附件 3

## 答標對照表：

項次	規格內容	廠商所投規格(廠商填寫)		審核(本中心填寫)	
		佐證資料中規格描述	頁次		
1		<input type="checkbox"/> 完全符合： <input type="checkbox"/> 優規：		<input type="checkbox"/> 符合	
				<input type="checkbox"/> 不符合	<input type="checkbox"/> 無佐證資料 <input type="checkbox"/> 資料規格不符 <input type="checkbox"/> 資料無法佐證 <input type="checkbox"/> 資料無法判定 <input type="checkbox"/> 其它：_____ _____