**114年第二次電腦軟體共同供應契約採購-雲端服務**

**(1140202)** **雲端服務檢核表**

雲端微服務(SaaS)辧公室生產力工具(含郵件、行事曆、 雲端硬碟、即時通等)共通性資通安全基本要求

|  |  |
| --- | --- |
| 雲端服務名稱 | AaaS 雲端服務 |
| 資料或系統類型 | ■符合【普】資料或系統類型(所有【普】標示為●之項目皆須符合並進行說明，其他則為選填)  ■ 符合【中】、【高】資料或系統類型(所有項目須符合並說明) |

以下為「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(112.9.25版)」中，要求【普】或【中】、【高】類型之資料或系統類型應建議辦理之各項控制措施。

請投件廠商依本檢核表，就所提之雲端服務產品實際情形，勾選【普】或【中】、【高】資料或系統類型，並於「廠商說明欄」填覆相關對應措施，**本表格內容後續將公告於資訊服務採購網中。**

填寫說明：

1. 圖示表示：● 建議辦理，◎ 經訂購機關評估個案有必要時辦理，▲ 依訂購機關資通安全責任等級辦理。
2. 普、中、高皆標示 ◎ 項目(橘色項目)，為所有廠商選填項目，提供機關個別評估時參考。

| **項目** | **子項** | **資料或系統類型** | | | **請廠商自我檢視並填寫相關說明**  填寫日期：中華民國 113年 11 月 22日 |
| --- | --- | --- | --- | --- | --- |
| **高** | **中** | **普** |
| 提供服務商 | 須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準 | ● | ● | ● | **■ 符合要求：**  雲端服務應具備以下三項資訊安全管理制度及雲端服務個人資訊保護相關國際或國家標準驗證(通過驗證之證明文件須顯示出雲端服務在驗證範圍內，雲端服務原廠得以合作之公有雲業者通過驗證證書代之)：   1. 資訊安全管理系統國際標準(ISO/IEC 27001)或國家標準(CNS 27001)，二者擇一。 2. 雲端服務資訊安全管理國際標準，如ISO/IEC 27017或雲端安全聯盟CSA Star(等級不限)等，二者擇一 3. 雲端服務個人資訊保護管理國際標準(ISO/IEC 27018)。   鎧睿全球科技取得 ISO27001:2022 認證，AaaS 雲端服務建置於台灣智慧雲端服務公司(簡稱台智雲)，其 IDC 機房服務通過多項國際認證標準，能滿足客戶機密性、完整性、可用性規範之需求。  https://tws.twcc.ai/cloud-security/ |
| 須通過CNS 27701或ISO 27701等隱私資訊管理標準、其他具有同等或以上效果之系統或標準  (提供服務項目涉及個資時機關應納入要求) | ◎ | ◎ | ◎ | (為訂購機關依個案評估有必要辦理時參考，廠商自行選擇是否填寫或提供，有證書提供者將於資訊服務採購網中揭露) |
| 不得為大陸地區廠商或第三地區含陸資成分廠商 | ● | ● | ● | **■ 符合要求：**   1. 雲端服務原廠不得為「中國大陸（含港、澳）地區廠商」或「經濟部投資審議委員會列為陸資來台投資事業名錄之廠商」者。 2. 經數位發展部資通安全署、國家安全會議及其他資安、國安等機關通知有資安疑慮，例如投件廠商、投件代理商所提供產品之原廠屬「第三地區含陸資成分廠商」。   鎧睿全球科技為資通安全自主產品在臺附加價值率 100% 之系統原廠，定期申請/通過數位發展部數位產業署推動的資訊安全能量登錄暨資通安全自主產品認定。  https://www.cisanet.org.tw/News/Detail/5957 |
| 傳輸機密性與完整性 | 廠商提供機關資料傳輸措施 | ● | ● | ● | **■ 符合要求：**  請詳閱雲端服務安全性檢測個案編號CS-001：雲端服務均須具備「傳輸層安全通訊協定(Transport Layer Security-TLS)」的安全通訊協定v1.2以上。  應用系統服務皆強制使用 TLS v1.2 以上傳輸協定。 |
| 事件日誌保存與可歸責性 | 應提供日誌保存，包括記錄帳號與權限變更、登入名稱、時間、IP 位址、資料存取及重要安全性事件等，應確保其完整與正確性並符合機關保存年限(建議至少六個月)要求 | ● | ● | ● | **■ 符合要求：**  **依雲端服務共契採購契約要求**，雲端服務與履約標的相關之日誌保存項目如下：   1. 應用程式日誌(AP log)**(必要)** 2. 登入日誌(logon log)**(必要)** 3. 網站日誌(web log)**(必要)** 4. 作業系統日誌(OS event log)：若無法提供請提出說明(例如:因服務底層採用Serverless等架構，無直接管理作業系統，故無法提供作業系統日誌。)   上述日誌項目保存期限：自資料產生起保存**至少6個月**(含契約終止或解除或期滿後)。  系統主控台具各類型日誌查詢及設定保留期限(已符合至少保留 6 個月之規範)，各類日誌包含：  安全 Webmail 日誌 (imaps.log) 包含應用程式日誌、網站日誌；登入日誌 (ldap.log)、認證日誌 (auth.log)、系統日誌 (syslog)、安全日誌 (sshd.log)… |
| 供應商及產品安全要求 | 針對供應商、產品之下列要求提出佐證資料，若無符合條件者提請機關資安長確認風險 1.供應商安全：符合以下**任一**條件。  (1)廠商有公開漏洞回報應變機制  (2)廠商有第三方檢測團隊執行檢測  2.產品安全：符合以下**任一**條件。  (1)產品經第三方檢測單位未含OWASP TOP 10弱點之報告  (2)提供經商用弱點檢測軟體未含**中、高**等級風險之掃描報告  (3)取得第三方認可實驗室認證，如：行動應用App基本資安標章（Mobile Application Basic Security,MAS）、Common Criteria或其他同等級認證 | ● | ● | ● | **■ 符合要求：**   1. 供應商(雲端服務原廠)安全   **■** 漏洞回報應變機制：  (請廠商依據左列說明漏洞回報與應變之機制)  本公司遵循 ISO27001 與資通安全事件通報及應變辦法，並且主動通報利害關係者。  相關流程已明訂於「ISMS-2-00016 資訊安全事故管理作業標準\_v1.4」，如發現已知漏洞除發送郵件通知外，於客戶用 FAQ 亦會公告相關漏洞資訊。    **■** 有第三方檢測團隊執行檢測：  (如有第三方檢測團隊協助，請提供相關資訊)  由雲端共契弱點掃描檢測。   1. 產品安全 2. 請詳閱雲端服務安全性檢測個案編號CS-002(OWASP TOP 10 最新版應用程式弱點掃描) 3. 請詳閱雲端服務安全性檢測個案編號CS-003(系統弱點掃描) 4. □本雲端服務提供App，並已取得行動應用App基本資安標章。   App名稱：請填版本號  □Android：請填版本號  □iOS：請填版本號 |
| 廠商通過網路安全成熟度模型認證(Cybersecurity Maturity Model Certification, CMMC) | ◎ | ◎ | - | (為訂購機關依個案評估有必要辦理時參考，廠商自行選擇是否填寫) |
| 防惡意軟體 | 靜態分析 | ● | ● | ● | (符合【普】、【中】、【高】者必填，請廠商依據左列具體說明雲端服務具備防惡意軟體之靜態分析機制)  AaaS 雲端服務具備 APT 惡意程式行為靜態分析機制，包含：反偵測行為、CVE 弱點漏洞偵測、加密演算行為、嵌入漏洞檢查套件、隱藏包裝、文字命令程式、郵件識別、惡意文件、惡意程式、手機惡意程式、惡意網址等。 |
| 動態沙箱分析 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列說明雲端服務具備防惡意軟體之動態沙箱分析具體機制)  AaaS 雲端服務具備 APT 惡意程式行為動態沙箱分析機制，於沙箱環境動態執行程式取得沙箱日誌後，再執行 APT 惡意程式行為分析機制包含：反偵測行為、CVE 弱點漏洞偵測、加密演算行為、嵌入漏洞檢查套件、隱藏包裝、文字命令程式、郵件識別、惡意文件、惡意程式、手機惡意程式、惡意網址等。 |
| 防惡意連結 | 靜態分析 | ● | ● | ● | (符合【普】、【中】、【高】者必填，請廠商依據左列具體說明雲端服務具備防惡意連結之靜態分析機制)  AaaS 雲端服務提供釣魚網址資料庫比對、內容過濾分析引擎 (繁體/簡體/英文/主旨/內文/附件/超連結)、HTML 內文清理清除不合乎 HTML 規範與可能有害內容、阻擋 URL，在用戶點及連結前再次提醒等機制。 |
| 動態沙箱分析 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列具體說明雲端服務具備防惡意連結之動態沙箱分析機制)  AaaS 雲端服務具備 APT 惡意連結動態沙箱分析機制，於沙箱環境動態執行惡意連結取得沙箱日誌後，再執行 APT 惡意程式行為分析機制包含：反偵測行為、CVE 弱點漏洞偵測、加密演算行為、嵌入漏洞檢查套件、隱藏包裝、文字命令程式、郵件識別、惡意文件、惡意程式、手機惡意程式、惡意網址等。 |
| 防釣魚郵件 | 釣魚郵件過濾 | ● | ● | ● | (符合【普】、【中】、【高】者必填，請廠商依據左列具體說明雲端服務具備釣魚郵件過濾機制)  藉由 3000+ 萬已知駭客 IP 地址與短期快閃釣魚網址資料庫，以及主動式未知釣魚誘餌防禦：包含假冒、匿名、濫發、非法、亂數、中間人、共用、公有雲行為解析攔截，APT 釣魚誘餌郵件與 BEC 商業詐騙郵件。ArmorX APT 主動式未知釣魚誘餌防禦是全球最前瞻的先發性即時行為偵測技術，是企業「制敵於先 · 新招必剋」的最佳利器。 |
| 身分偽冒辨識(anti-spoofing) | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列具體說明雲端服務具備身分偽冒辨識機制)  運用全球獨家專利技術「SMTP 即時回溯追蹤」與「SMTP 駭客行為解析」，在 SMTP 交握階段即可有效辨識濫發、非法、匿名、偽造等寄件行為，攔截變臉詐騙與惡意郵件行為。 |
| 資料與個資  安全 | 資料分類與標籤 | ● | ● | ● | (符合【普】、【中】、【高】者必填，請廠商依據左列具體說明雲端服務之資料分類與標籤做法)  AaaS 雲端服務提供資料分類與標籤機制。個資辨識包含預設標準個資、自訂行為個資、自訂排除個資；比對方式支援精準檢驗公式、正規表示式、關鍵字。  標準個資的精準程式檢驗由系統提供，例如信用卡卡號、身份證字號；個別行業行為個資的精準檢驗公式，例如銀行帳號、保險單號，由企業提供後置入系統；支援排除標題個資、去重複計算。 |
| 資料加密與存取控制 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列分別具體說明雲端服務資料加密與存取控制之做法)  本系統是自有專用 OS 高安全、高效率，  反竄改、(入侵)程式異動加密封鎖，  無 Root 密碼，以 4K 環境因子、PKI 金鑰密碼存取。  租戶端以 HTTPS 加密連線方式，使用帳號/密碼登入管理介面，帳號權限為網域管理者僅提供簡易管理。  透過系統權限控管、授權帳號權限身分，僅符合此身分權限的帳號才可查詢授權資料。 |
| 資料外洩防護 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列具體說明雲端服務如何防止資料外洩做法)  AaaS 雲端服務提供 DLP 電子郵件稽核加密服務，透過規則設定，可防止機關定義的機敏資料或個人資料外洩。 |
| 未經機關審查同意，不得將雲端資訊系統或儲存資料移至本國以外地區 | ● | ● | ● | **◼符合要求：**  **依雲端服務共契採購契約要求**，雲端服務資料儲存所在地於本國境內者，未經機關審查同意不得隨意變更至本國境外。  AaaS 雲端服務建置於台灣智慧雲端服務公司(簡稱台智雲)，其公司所營運雲服務係建構於國家高速網路與計算中心的國家級 AI 研發與雲端服務基礎設施，主資料中心坐落於台中分部，並以台南分部作為備援資料中心。 |
| 資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。 | ● | ● | ● | **◼符合要求：**  **依雲端服務共契採購契約要求**，雲端服務資料存取、備份及備援之實體機房所在地不得位於中國大陸（含港、澳），且不得跨該等境內傳輸相關資料。 同上。 |
| 廠商對於虛擬主機平台內之虛擬主機映像檔，應強化其儲存與使用安全並提供佐證 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列說明提供具體做法及佐證。)  AaaS 雲端服務建置於台灣智慧雲端服務公司(簡稱台智雲)，其平台支援 [openstack](https://specs.openstack.org/openstack/cinder-specs/specs/zed/image-encryption.html) 映像檔加密機制，ArmorX 於台智雲安裝之虛擬運算個體，選用加密資料磁碟，系統以進階加密標準 (AES-256) 演算法加密磁碟資料，可確保資料安全。  可參考台智雲提供之手冊：https://docs.twcc.ai/docs/user-guides/twcc/vcs/vds/create-encrypted-data-disks/ |
| 身分驗證與  存取控制 | 多因子認證 | ● | ● | ● | (符合【普】、【中】、【高】者必填，請廠商依據左列具體說明雲端服務之多因子認證做法)  AaaS 雲端服務 OTP 動態密碼認證機制。 |
| 零信任：身分鑑別/設備鑑別/信任推斷 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列具體說明雲端服務之零信任：身分鑑別/設備鑑別/信任推斷做法)  Web Mail 提供帳號/密碼、OTP 認證，並提供登入日誌識別身份，列表包含登入時間、來源 IP、來源國碼、作業系統、瀏覽器    APP 支援  行動裝置控管和登入記錄    登入時間、來源 IP、來源國碼、作業系統、版本、裝置名稱 |