**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 | 郵件稽核系統 |
| 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 11 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)。 |
| 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) | ◎ | ◎ | ◎ | 公有雲業者已通過 ISO 27701驗證。 |
| 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」。 |
| 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。 |
| 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)：**需稽核的信件會先進入稽核主機進行條件檢查，若符合條件會進行設定的動作，所以保留稽核主機的稽核紀錄6個月。 2. 登入日誌(logon log)**(必要)：**管理者登入系統後台設定稽核條件及動作，所以保留管理者登入系統的登入紀錄，另使用者登入Webmail審核被稽核的信件，所以也保留有審核權限的郵件帳號登入Webmail的登入紀錄，兩者皆保留6個月。 3. 網站日誌(web log)**(必要)：**保留管理者後台與Webmail的網站日誌6個月。 4. 作業系統日誌(OS event log)：稽核主機負責信件的稽核運算，所以保留稽核主機的作業系統紀錄6個月。   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)。 |
| 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)  **■** 有第三方檢測團隊執行檢測：已於113年第六次電腦軟體共同供應契約採購-雲端服務(1130206)通過弱掃檢測。   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：請填本雲端服務提供之App名稱  □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 | ● | ● | ● | 本系統採用防毒軟體多層式防護，防範持續性及針對性攻擊，以及勒索病毒和其他類型的零時差惡意程式。 |
| 動態沙箱分析 | ● | ● | ◎ | 本系統針對信件的附檔進行分析偵測，壓縮檔會先解壓縮再進行偵測，附檔若符合系統病毒資料庫相關特徵值，將先移至專屬帳號隔離處理。(額外收費項目) |
| 防惡意連結 | 靜態分析 | ● | ● | ● | 本系統比對國際黑名單並依危害等級標示不同分數，符合信件可增加警告標記、將信件直接送至垃圾郵件資料夾或退信。 |
| 動態沙箱分析 | ● | ● | ◎ | 本系統具備網址改寫功能，可以針對所有網址或符合系統內建條件的可疑網址，將郵件夾帶的連結指向專屬頁面，且系統會提示阻攔，避免使用者存取。(額外收費項目) |
| 防釣魚郵件 | 釣魚郵件過濾 | ● | ● | ● | 本系統偵測信件表頭與內文以及信件寄送行為等特徵，檢查多筆黑名單，給予標記與分數作為釣魚信件判斷依據。 |
| 身分偽冒辨識(anti-spoofing) | ● | ● | ◎ | 本系統採用SPF、DKIM、DMARC等標準驗證，整合全球詐騙威脅情資黑名單，比對檢查郵件中標頭內容、顯示名稱，防範網域冒用、郵件標頭偽造及相似網域詐騙。 |
| 資料與個資  安全 | 資料分類與標籤 | ● | ● | ● | 本系統將用戶往來的資料會區分為一般資料及機敏機料，機敏的資料除系統預設的個資格式外，可於稽核條件處彈性添加分類標籤。 |
| 資料加密與存取控制 | ● | ● | ◎ | 本系統可依據標籤動態調整控制存取權限，包含套用分類標籤、附檔自動加密與禁止資料傳送(收發信)，並支援S/MIME 加密及ZIP 壓縮檔加密。 |
| 資料外洩防護 | ● | ● | ◎ | 本系統能夠檢測出郵件內容和附件中的機敏資料，例如個資中的身分證、信用卡號碼等，以及自訂的敏感關鍵字。一旦偵測到符合的資料，系統會根據設定的政策進行相應動作，包括阻止郵件發送、發出警告、轉發或加密附件，避免資料不當洩漏。 |
| 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。 |
| 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。 |
| 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 | ● | ● | ◎ | 本系統的虛擬機(VM)映像檔會自動化定時備份，因應災難還原需求並留存紀錄。  佐證如下 :  1. 系統快照截圖    2. 系統負載平衡器截圖    3. 資料備份截圖 |
| 身分驗證與  存取控制 | 多因子認證 | ● | ● | ● | 本系統登入均結合Google Authenticator兩階段驗證。 |
| 零信任：身分鑑別/設備鑑別/信任推斷 | ● | ● | ◎ | 身份鑑別：搭配手機進行兩階段驗證  設備鑑別：24小時監控郵件稽核伺服器，確保第一時間發現異常並處理。 |