**113年第六次電腦軟體共同供應契約採購-雲端服務**

**(1130206)** **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

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】、【中】及【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為【普級】或【中】、【高】資料或系統類型，併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。**

服務名稱：　M+服務圈

■符合【普級】資料或系統類型(所有「高、中、普」標記●項目，皆須符合並進行說明，標記「高、中」標記●項目，則為選填)

■符合【中】、【高】資料或系統類型(所有項目皆須符合並進行說明)

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辦理時，▲ 依訂購機關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 月 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) | ◎ | ◎ | ◎ | 已通過 |
| 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 | ● | ● | ● | **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)**   日誌儲存於地端與日誌查詢服務ELK上，包含時間與可查詢流水號，資料保存至少半年   1. 登入日誌(logon log)**(必要)**   登入日誌儲存於資料庫，包含帳號、登入時間與權限變更紀錄，資料保存半年以上   1. 網站日誌(web log)**(必要)**   日誌儲存於地端與日誌查詢服務ELK上，包含時間與可查詢流水號，資料保存至少半年   1. 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。)   使用SOC作監控，只要登入作操作就會將操作行為連同帳號、ip與登入時間送出，特定安全事件同樣會送出，涵蓋作業系統日誌  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   ■有第三方檢測團隊執行檢測：財團法人台灣商品檢測驗證中心   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 TOP10 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，並取得行動應用App基本資安標章。App名稱：M+ Messenger   ■ Android：7.4.005 ■ iOS：7.4.005 |
| 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 | ● | ● | ● | 軟體更版皆執行並產稱弱點掃描報告與第三方library高風險評估報告，確保無惡意軟體注入風險 |
| 動態沙箱分析 | ● | ● | ◎ | 主機定期進行弱掃並產生弱掃報告，確保無高風險弱點導致惡意軟體注入風險 |
| 防惡意連結 | 靜態分析 | ● | ● | ● | 軟體更版皆執行並產稱弱點掃描報告與第三方library高風險評估報告，確保無惡意連結相關的高風險 |
| 動態沙箱分析 | ● | ● | ◎ | 主機定期進行弱掃並產生弱掃報告，確保無高風險弱點導致惡意連結相關高風險 |
| 防釣魚郵件 | 釣魚郵件過濾 | ● | ● | ● | 非郵件軟體，不適用 |
| 身分偽冒辨識(anti-spoofing) | ● | ● | ◎ | 非郵件軟體，不適用 |
| 資料與個資  安全 | 資料分類與標籤 | ● | ● | ● | 已進行資料分類與標籤，通過ISO27701  實際方式為建立系統個資清冊，包含以子系統作為分類，每個分類使用的個資項目，使用既定標籤歸類使用個資項目分數，並計算風險等級，根據風險等級訂定防護措施 |
| 資料加密與存取控制 | ● | ● | ◎ | 已進行資料加密與存取控制，通過ISO27701  會根據具有個資的儲存資料表，計算風險分數，評估風險分數是否高於閥值並進行降低，監控具有個資的資料表，若有帳號存取則記錄並告警  資料存取時限制並記錄存取對象，資料存取採用https加密傳輸、若資料匯出，資料落地後皆進行密碼防護，密碼長度6以上並包含英數字 |
| 資料外洩防護 | ● | ● | ◎ | 已進行資料外洩防護，通過ISO27701  線上資料傳輸皆進行Https加密，cipher皆為高安全等級，下載儲存的資料落地後皆進行密碼防護，密碼長度6以上並包含英數字 |
| 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：**  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：**  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 | ● | ● | ◎ | VM主機非使用映像檔備份，採HA架構多VM跨實體主機提供服務，另定期將VM內重要資料夾進行異地備份，異地端僅有OM可進行存取，同樣採多因子驗證  1. 設定Identity and Access Management 機制來限制對異地備份檔的存取  2. 定期清理不再使用或過期的備份檔，以減少攻擊面並防止舊備份檔洩漏的風險 |
| 身分驗證與  存取控制 | 多因子認證 | ● | ● | ● | 符合，登入需進行多因子驗證，使用輸入帳密前需使用MOTP做OTP驗證，另外所有操作皆由跳板機進行並錄製操作 |
| 零信任：身分鑑別/設備鑑別/信任推斷 | ● | ● | ◎ | 符合，登入需進行多因子驗證，使用輸入帳密前需使用MOTP做OTP驗證，另外所有操作皆由跳板機進行並錄製操作 |