**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 | Meeting Ink 會議記錄軟體 |
| 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 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) | ◎ | ◎ | ◎ | (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」。 |
| 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)** 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)：   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：  目前由外部的客服管道 (email, FB)讓使用者回報以及內部定期掃描檢測，再轉由產品與工程單位處理。依照確認漏洞對應至工程單位做開票並與工程修復。  **🗹**有第三方檢測團隊執行檢測：執行之檢測為”伺服器主機安全檢視報告” (如附件一)，執行廠商為”竣盟科技股份有限公司”。   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或提供，有證書提供者將於資訊服務採購網中揭露) |
| 防惡意軟體 | 靜態分析 | ● | ● | ● | 本服務於前端軟體中實施靜態分析，針對應用程式的程式碼結構進行全面檢測，以防範潛在的惡意軟體或安全漏洞。委外資安顧問公司分析涵蓋Meeting Ink 應用程式的項目包含敏感性資料的洩漏、程式碼中不應存在的敏感性資訊、以及潛在的注入攻擊風險。此外，透過分析軟體引用的函式庫及其更新狀態，能確保第三方資源不引入安全隱患。我們亦檢查應用程式中實施的加密機制是否符合現代標準，以保障敏感性資料的儲存及傳輸安全。靜態分析有助於在應用程式發布前即時發現安全漏洞，提升整體軟體的安全性與信任度。 |
| 動態沙箱分析 | ● | ● | ◎ | 本服務於前端軟體執行時實施動態分析，以模擬實際使用情境，深入檢測潛在的惡意行為及安全隱患。委外資安顧問公司分析涵蓋Meeting Ink 應用程式的資源調用、敏感性資料的存取與傳輸，並主動記錄交易資源的使用情形。我們檢測應用程式是否可能在運行期間暴露敏感性資料於記憶體、日誌檔案或不安全區域，並確保未經授權的行動應用程式無法存取分享資料。此外，動態分析還監控系統資源的使用狀況，確保伺服器憑證有效性與用戶操作權限無異常。此過程確保應用程式在運行中符合安全性需求，避免潛在攻擊風險。 |
| 防惡意連結 | 靜態分析 | ● | ● | ● | 本雲端服務僅整合Azure服務連結與迪威自有雲連結，並透過CSP設置服務僅使用上述連結做使用範圍 |
| 動態沙箱分析 | ● | ● | ◎ |  |
| 防釣魚郵件 | 釣魚郵件過濾 | ● | ● | ● | 本服務無郵件服務提供 |
| 身分偽冒辨識(anti-spoofing) | ● | ● | ◎ | (同上) |
| 資料與個資  安全 | 資料分類與標籤 | ● | ● | ● | 本服務採用Azure雲端服務提供數據隔離，Azure是多租用戶服務，這表示多個客戶部署和VM會儲存在相同的實體硬體上但會透過Azure邏輯做資料訪問的區隔。並且本服務同樣使用邏輯隔離來區隔每位客戶的儲存資料，設置同時嚴格權限防止客戶存取彼此的數據。迪威目前之Meeting Ink 會議記錄服務上述功能皆有使用。  基於上述架構，目前系統將用戶標籤分為三類:  -分類1: Super admin  具有此標籤之用戶為廠商之後台管理者。具備新增機關帳號、新增機關帳號下之機關用戶、刪除用戶、查看屬於此機關用戶之總用量權限。  -分類2: Admin:  具有此標籤之用戶為機關內部系統管理者,具有新增機關帳號下之機關用戶、刪除用戶、查看屬於此機關用戶之總用量權限。但不具備查看單一用戶之資料權限。  -分類3: 一般用戶  此類用戶具備Meeting Ink產品基本功能使用之權限如: 錄音、錄音轉逐字稿、逐字稿產出摘要、逐字稿產出翻譯等功能之權限。但不具備查看其他用戶，或機關admin之相關權限。 |
| 資料加密與存取控制 | ● | ● | ◎ | Microsoft提供許多選項，可供客戶用來保護 Azure 網路內部內部傳輸中的數據，以及透過因特網外部傳送給終端使用者。 其中包括透過虛擬私人網路 (利用 IPsec/IKE 加密) 與傳輸層安全性 (TLS) 1.2 或更新版本 (透過 Azure 元件，例如應用程式閘道或 Azure Front Door) 進行通訊，以及直接在 Azure 虛擬機器上 (例如 Windows IPsec 或 SMB) 的通訊協定進行通訊等等。迪威目前之Meeting Ink 會議記錄服務上述功能皆有使用。 |
| 資料外洩防護 | ● | ● | ◎ | Azure資料庫服務受控執行個體可提供稽核和威脅偵測功能，以保護客戶資料。具有Azure監視器記錄和事件審核、紀錄系統，可分析您的記錄，以偵測不尋常的行為、可能有害的存取或惡意探索資料庫等嘗試。 系統會建立可疑活動警示，例如：SQL插入、潛在資料滲透及暴力密碼破解攻擊，或存取模式發生異常等，以便攔截提升權限、入侵使用認證等情況。 而資料庫會新增一層安全性來協助保護待用資料，以免原始檔案或備份遭到未經授權或離線存取。 常見的案例包括資料中心遭竊或不安全的硬體或媒體 (例如磁碟機和備份磁帶) 處置方式。TDE 會使用 AES 加密演算法將整個資料庫加密，應用程式開發人員不需對現有的應用程式進行任何變更，以防護線上與實體外洩的情形。迪威目前之Meeting Ink 會議記錄服務上述功能皆有使用。 |
| 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 | ● | ● | ◎ | 本服務虛擬主機平台內皆已配合委外資安公司設置政府組態基準(GCB)，迪威目前之Meeting Ink 會議記錄服務運行於該設置之虛擬主機，符合政府資通訊設備規範，以降低成為駭客入侵管道。佐證資料請詳本份文件之 ”附件一”。 |
| 身分驗證與  存取控制 | 多因子認證 | ● | ● | ● | 本服務內部後台系統透過Microsoft Entra做身份管理，並使用該服務的多因子認證綁定裝置。 |
| 零信任：身分鑑別/設備鑑別/信任推斷 | ● | ● | ◎ | 同上多因子認證敘述，透過內部管理強制採用MFA並綁定員工的移動裝置做零信任驗證。每個身份訪問權限皆遵守最小權限原則，並且做定期密碼輪替。 |

**附件一:**

說明: 附件一為針對雲端服務檢核表: “資料與個資安全 - 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” 項目之佐證. 附件圖檔僅提可佐證部分，避免公司內部系統資訊洩漏請見諒一張含有 文字, 螢幕擷取畫面, 字型, 數字 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 數字, 字型 的圖片

自動產生的描述