**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：源思科技雲端即時通

□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 07 月08 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)。   源思科技之資通安全管理措施通過ISO 27001標準，有效證書如下： |
| 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」。   源思科技在經濟部商業司(24765217)的公示資料登記如下： |
| 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。並已關閉不安全的演算法。 |
| 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)** 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)。  Log皆有備份於雲端空間，佐證如圖。 |
| 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)  依照左欄子項No1敘述「1.供應商安全：符合以下任一條件。」。因我們每年請第三方進行檢測，並在此次提交報。所以有符合之。  **🗹**有第三方檢測團隊執行檢測：請提供第三方檢測團隊資訊  委請**關鍵智慧科技**有限公司進行滲透測試。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)   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： Juiker 請填本雲端服務提供之App名稱  □ Android： MAS-3752-11200014  請填版本號  □ iOS： MAS-3752-11200015 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，請廠商依據左列說明雲端服務具備防惡意軟體之靜態分析機制)  源思科技員工之Windows電腦皆有啟用Windows Defender，並安裝Avast Business防毒軟體(包含MacOS)。伺服器端應用程式每月進行套件相依性掃描。Juiker提供企業用戶為加密傳輸方案，使用者於聊天室內傳輸之檔案(client端加密後特徵已破壞)，無法傳至第三方進行靜態分析。建議企業管理者設定允許傳輸之檔案類型白名單，例如封鎖exe, zip, msi 等執行檔。 |
| 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機制)  Juiker提供企業用戶為加密傳輸方案，使用者於聊天室內傳輸之檔案(client端加密後特徵已破壞)，無法傳至第三方進行動態沙箱分析。  員工應利用本地電腦態沙箱分析軟體掃描後，在透過Juiker傳送給群組。 |
| 防惡意連結 | 靜態分析 | ● | ● | ● | (符合【普】【中】、【高】者必填，請廠商依據左列說明雲端服務具備防惡意連結之靜態分析機制)  與趨勢科技合作進行惡意連結掃描，未曾造訪過之連結一律採靜態掃描後紀錄分數，第二次造訪直接以網址進行吻合(一律阻擋, 不再分析)。 |
| 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連結之動態沙箱分析機制)  與趨勢科技合作進行惡意連結掃描，未曾造訪過之連結一律採動態掃描後紀錄分數，第二次造訪直接以網址進行吻合(一律阻擋, 不再分析)。 |
| 防釣魚郵件 | 釣魚郵件過濾 | ● | ● | ● | (符合【普】【中】、【高】者必填，請廠商依據左列說明雲端服務具備釣魚郵件過濾機制)  不適用，本服務不提供郵件收發。若為釣魚連結同上由趨勢科技判斷URL使否已為黑名單。 |
| 身分偽冒辨識(anti-spoofing) | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列說明雲端服務具備身分偽冒辨識機制)  企業會員身份採實名制，且於頭像會有光圈，並且身份資料由企業之AD Server控制並產生連動，企業會員無法自行設定顯示名稱。如果職稱或部門發生異動，也會隨之異動在App內顯示之身份。 |
| 資料與個資  安全 | 資料分類與標籤 | ● | ● | ● | (符合【普】【中】、【高】者必填，請廠商依據左列說明雲端服務之資料分類與標籤做法)  根據ISO 27001:2022(5.9)標準之要求，依照資訊資產管理作業流程進行資料分類與標籤。 |
| 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說明雲端服務資料加密與存取控制之做法)  用戶端APP於首次安裝時產生隨機密碼用於加密行動端資料庫，需透過Missed Call來電或是簡訊驗證。APP與後台傳輸訊息使用TLS 1.2加密通道取得1小時Token後，以Token存取包含訊息/通話/視訊等服務。訊息傳送至後台時另外的金鑰進行加密(At rest encryption)後儲存於分散式資料庫。  APP通話採用SRTP加密聲音封包。  使用者登入電腦版之密碼採用雜湊函式後儲存於資料庫。 |
| 資料外洩防護 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列說明雲端服務如何防止資料外洩做法)  源思科技雲端即時通，後端SSH主機連線均須先連上VPN並於登入時進行OTP二次驗證。主機之間禁止橫向移動，只允許由指定入口主機進行版本更新部署。    主機登入紀錄與維運人員輸入指令，均以Log Server進行偵測和告警。 |
| 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。  資料儲存於台灣固網台北機房。 備援指定儲存於GCP彰濱工業區。 |
| 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。  資料儲存於台北台灣固網機房。備援指定儲存於GCP彰濱工業區。 |
| 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，請廠商依據左列分別說明雲端服務於虛擬主機平台內之虛擬主機映像檔強化儲存與使用安全做法)  源思科技雲端即時通，採用Rocky Linux與Ubuntu LTS版，每次應用程式版本異動後，皆有進行主機映像檔備份。  本系統安全性的OS Hardening步驟：   1. 保持系統更新： 2. 加強 SSH 存取安全：    * 禁用 root 登入    * 更改預設的 SSH 連接埠    * 使用MOTP兩階段驗證套件 3. 配置防火牆：    * 使用 firewalld 或 iptables 限制傳入連接只允許關聯的服務互相連接，主機與主機之間無法連接。 4. 實施強密碼策略：    * 強制執行密碼複雜度和過期政策 5. 禁用不必要的服務：    * 移除或禁用不需要的服務 6. 保護使用者帳戶：    * 實施最小權限原則    * 每年審核使用者帳戶和權限並移除使用者 |
| 身分驗證與  存取控制 | 多因子認證 | ● | ● | ● | (符合【普】【中】、【高】者必填，請廠商依據左列說明雲端服務之多因子認證做法)  對於多因子認證，提供多種選項以增強安全性：   1. 註冊流程：    * 使用未接來電的末四碼作為驗證碼    * 或者透過簡訊（SMS）發送驗證碼 2. 密碼變更：    * 變更密碼時，同樣需要進行上述驗證步驟之一 3. 電腦版登入：    * 需要使用手機應用程式（APP）接收一次性密碼（OTP）    * 此 OTP 將在應用程式內生成，用於完成登入程序 |
| 零信任：身分鑑別/設備鑑別/信任推斷 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列說明雲端服務之零信任：身分鑑別/設備鑑別/信任推斷做法)  身分鑑別: 包含三個部分。  一，公私分離，私人帳號如同前述使用MissedCall或SMS進行驗證，但企業帳號身份資料俱來自AD Server。企業帳號僅能由企業內部信箱使用APP進行QRCode掃瞄開通，開通後需設定電腦版密碼，於後續登入時使用用以自證身份。或由管理者自後台強制為所有員工設定企業帳號/密碼。  二，顯示名稱，員工無法自行設定/偽造顯示名稱。  三，聊天室成員清單，由管理人員設定，從企業通訊錄或組織階層結構拉人成立。    設備鑑別: 每個登入裝置APP或電腦版均於首次啟動時產生一識別碼紀錄於後台。企業管理者可於頁面查看登入之裝置歷程。管理平台可更進一步限制使用者可允登MAC Address。 |