**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 | U通訊 |
| 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 25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)。 2. 雲端服務資訊安全管理國際標準 ISO/IEC 27017。 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**，機關用戶於U系統有以下重要活動時，均紀錄於日誌供查核檢閱：   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)。   U系統同時也使用雲端服務供應商所提供的整合介面，收集維運安全日誌，並在發生異常狀況時通知相關人員介入處理。 |
| 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：本產品設有公開回報機制，使用者遇使用上疑難可直接於產品內回報問題，並由原廠協助處理。  □有第三方檢測團隊執行檢測：   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：U Messenger  **☑**Android：7.17.2  **☑**iOS：7.17.2 |
| 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 | ● | ● | ● | 使用者透過U上傳或下載檔案時，伺服器提供以下機制確保檔案安全：  1. 檔案須通過防毒軟體及威脅防護軟體掃描無病毒及威脅檢出  虛擬主機內安裝防毒及威脅防護軟體並定期更新病毒碼，防毒及威脅防護軟體即時監控主機是否有病毒及威脅出現，當發現病毒或威脅時即時將病毒清除。檔案在上傳或下載時，執行檔案檢測服務以確保安全。  2. 檔案須通過完整性檢查  檔案在上傳或下載時，均須計算校驗碼並進行比對，比對結果須相同以確保檔案在傳輸過程中保有完整性，未經竄改或損毀。 |
| 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) |
| 防惡意連結 | 靜態分析 | ● | ● | ● | 當使用者於聊天群組中收到連結欲點開時，會彈跳提醒連結可能不安全，詢問是否確定要開啟。 |
| 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) |
| 防釣魚郵件 | 釣魚郵件過濾 | ● | ● | ● | 本產品非郵件服務，無須過濾釣魚郵件。 |
| 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) |
| 資料與個資  安全 | 資料分類與標籤 | ● | ● | ● | 訊連科技旗下服務符合ISO 27001規範，避免任何資訊洩露於網際網路；確實備份重要資料，系統運作不中斷。 |
| 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) |
| 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) |
| 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**，資料備份儲存地點：雲端服務資料備份之儲存地點即機房之所在地；主要服務機房Google Cloud Platform位於彰化濱海工業區，異地備援機房中華電信 HiCloud位於台北市信義區。 |
| 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：**  **依雲端服務共契採購契約要求**，訊連科技U服務所部署之伺服器均位於通過國際級資訊安全認證之IDC機房，其資料存取及備份是使用Google Cloud Platform (彰化濱海工業區) 和中華電信 HiCloud (台北市信義區)。 |
| 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，請廠商依據左列說明提供具體做法及佐證。) |
| 身分驗證與  存取控制 | 多因子認證 | ● | ● | ● | **U通訊APP版本須結合密碼和生物辨識**：  用戶在登入時需要輸入密碼後，也需另外使用Face ID（屬性因素）驗證身份後方可登入使用。 |
| 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) |