**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：ASUS WebStorage for Business

■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**  填寫日期：中華民國 113年06月27日 | | | **請廠商自我檢視並填寫相關說明** |
| --- | --- | --- | --- | --- | --- |
| **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 | ● | ● | ● | **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)。  提供佐證如下圖所示   * 應用程式日誌(AP log)、登入日誌(logon log)、網站日誌(web log)      * 作業系統日誌(OS event log) : |
| 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)  當發現漏洞回報事件，依照ISO27001與資通安全事件通報及應變辦法，並且主動通報利害關係者。其詳細流程已明訂於< ISMS-2-10 資訊安全事故管理作業程序書>之作業內容與程序，如下圖所示。    □有第三方檢測團隊執行檢測：請提供第三方檢測團隊資訊   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)   ■ 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：華碩雲端儲存雲(共契) 備註：新版審查中(2024-07-31)  ■ Android：華碩雲端儲存雲(共契) v3.11.3.2 ■ iOS：華碩雲端儲存雲(共契) v3.11.0.1 |
| 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)  採用的靜態分析機制是透過主動掃描所有上傳至雲端的檔案，包含程式碼、圖像、影音、文件等，來識別是否存在潛在的惡意軟體威脅。我們也會持續更新惡意軟體簽章，有效偵測並阻斷最新威脅，全面防護資料安全。 |
| 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)  當經由靜態分析結果，判斷檔案具惡意軟體威脅時，將會立即阻斷雲端用戶存取。 |
| 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)  本服務主要供應檔案雲端存取，不提供雲端用戶具有直接開啟外部連結功能之行為 |
| 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)  本服務主要供應檔案雲端存取，不提供雲端用戶具有直接開啟外部連結功能之行為 |
| 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)  本服務主要供應檔案雲端存取，不包含接收郵件之行為 |
| 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)  本服務主要供應檔案雲端存取，不包含接收郵件之行為 |
| 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)  雲端用戶可根據檔案重要程度來存放不同資料夾，例如專案類型檔案僅存放在專案資料夾內，個人檔案存放在私人資料夾內，達到資料分類與標籤。 |
| 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)  資料傳輸過程採 HTTPS 加密傳輸，儲存時去除檔案識別化，無法輕易辨識檔案類型，檔案存取權限僅雲端個人帳號使用，或授權的分享檔案。 |
| 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)  每個雲端用戶檔案存取權限僅限個人使用，除了用戶授權檔案給予他人使用除外，授權時可加上密碼、時效及次數限制。 |
| 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 | ● | ● | ◎ | (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)  本服務透過網路區域切割，限制授權的電腦且納入嚴格的帳號控管，達成虛擬主機存取與安全控管，其佐證如下圖所示。 |
| 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)  提供雲端用戶登入行為，除了帳號密碼驗證之外，還需要輸入一組驗證碼，以確保只有本人才能登入的帳戶。  用戶需要先進行帳號啟用雙重驗證功能的行為，並且選擇欲以下使用的驗證方式，依照指示完成設定。   * + 驗證器應用程式 : 使用受信任裝置上的應用程式 (例如 Google Authenticator) 產生驗證碼。   + Email驗證 : 接收Email傳送的驗證碼。   啟用雙重驗證後，用戶在行動裝置或瀏覽器上登入雲端用戶時，都需要完成驗證碼驗證，才可登入。  驗證碼驗證流程 :   * 輸入帳號和密碼。 * 根據先前設定的驗證方式，輸入或接收驗證碼。 * 完成驗證碼驗證後，即可登入 ASUS WebStorage。 |
| 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 : 於登入階段要求用戶先完成帳號、密碼認證，認證核可後，才可使用本服務 * 設備鑑別 : 透過啟用驗證器應用程式驗證(TOTP)，要求用戶只能使用受信任裝置上的應用程式，依其所產生的驗證碼，達成驗證登入 * 信任推斷 : 用戶可藉由查閱登入紀錄，依據登入時間、裝置、應用程式版本及IP位址等內容識別確認是否為可信任的登入行為 |