**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）套裝型

共通性資通安全基本要求

|  |  |
| --- | --- |
| 雲端服務名稱 | 雲端公文管理(Vital OD) |
| 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12 月20 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：**  Vital OD雲端服務建置於微軟 Azure 雲端服務平台，Azure 雲端服務平台具備所需證書如附件   1. 叡揚資訊\_ISO\_27001\_2013版證書(UKAS)\_2022.pdf 2. 叡揚資訊\_ISO\_27018\_2019版證書\_2022.pdf |
| 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) | ◎ | ◎ | ◎ | 本公司(叡揚資訊股份有限公司)具備 ISO 27701 證書如附件 1. 叡揚資訊\_ISO\_27701\_2019版證書\_2022.pdf |
| 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：**本公司(叡揚資訊股份有限公司)為台灣上櫃公司6752   1. 雲端服務原廠不得為「中國大陸（含港、澳）地區廠商」或「經濟部投資審議司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」。 |
| 身分鑑別/傳輸機密性與完整性 | 廠商提供機關帳號控管措施 | ◎ | ◎ | ◎ | (為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) |
| 廠商提供機關資料傳輸措施 | ◎ | ◎ | ◎ | 資料傳輸使用 https 加密傳輸，避免資料傳輸期間遭側錄或冒用 |
| 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)：無直接管理作業系統   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)。  服務使用微軟 Azure App Service 為 PaaS 平台。 |
| 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\_\_\_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：雲端供應商提供回報服務如下  <https://msrc.microsoft.com/create-report> 針對本系統若有異常或漏洞，則通知Vital OD的營運負責人員。並依照使用條款(參考如下)  (<https://www.gsscloud.com/tw/policies-terms>)  □有第三方檢測團隊執行檢測：  (如有第三方檢測團隊協助，請提供相關資訊)   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 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) |
| 資料安全 | 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。  本服務資料儲存於 Azure Japan (西日本) |
| 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。  本服務資料存於微軟Azure 西日本(主要備份儲存) 與東日本機房(Azure備援區域)，資料無跨提及區域大陸地區(含香港及澳門地區)傳輸。 |
| 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。) |