**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：　雲端電子郵件(EaaS)

□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 7 月 5 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)：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)。 |
| 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)  Openfind網擎資訊配合軟採辦預告之1130206契約條款將可能擬定的資安事件通報機制進行通報。通報過程大致為：廠商提供服務，如違反資通安全相關法令、知悉機關或廠商發生資通安全事件時，均必須於知悉時起1小時內通報機關及本共同供應契約訂約機關指定單位－數位發展部數位產業署軟體採購辦公室，提出緊急應變處置，並配合機關做後續適合之處理。  **☑**有第三方檢測團隊執行檢測：請提供第三方檢測團隊資訊  Openfind網擎資訊雲端服務有通過ISO27001國際認證，且歷年來皆通過雲端共契弱點掃描檢測無中高風險，雲端服務品質值得信賴。   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：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) |
| 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)  Openfind網擎資訊雲端服務具備 Sophos 防毒引擎與多道郵件過濾機制，可執行巨集及高風險檔案類型判斷、特徵值過濾、進階威脅偵測等，能有效判斷惡意威脅。可提供動靜態分析日誌，提供威脅事件資訊與檢測結果。 |
| 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)  Openfind網擎資訊雲端服務具備 Sophos 防毒引擎與多道郵件過濾機制，可執行巨集及高風險檔案類型判斷、特徵值過濾、進階威脅偵測、病毒特徵模型分析、更有APT動態沙箱分析機制，可偵測進階惡意程式，防止病毒偽裝 PDF 或 Office 檔並可模擬檔案在不同環境下是否有惡意變化等，能達到精準有效的惡意威脅判定。可提供動靜態分析日誌，提供威脅事件資訊與檢測結果。 |
| 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)  Openfind網擎資訊雲端服務能有效防止惡意連結，做好URL檢查避免使用者誤觸可疑連結，其中包含URL探索與分析、URL改寫機制，即時有效為使用者把關連結安全。 |
| 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連結之動態沙箱分析機制)  Openfind網擎資訊雲端服務能有效防止惡意連結，並達成進階動態防護，做好URL檢驗與阻擋、避免使用者誤觸可疑連結，其中包含URL探索與分析、URL改寫機制、即時比對全球網域及IP信譽列表、並提供動態連結風險偵測、降低利用使用差而導致的轉址攻擊風險，即時有效為使用者把關連結安全，有效達成動態進階社交工程防護。 |
| 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)  Openfind網擎資訊雲端服務具備完善郵件過濾機制，能即時比對國際化與在地化防詐騙智慧分析中心情資特徵、提供郵件灰名單機制、彈性化內容檢查。 |
| 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)  Openfind網擎資訊雲端服務具備完善郵件來源辨識技術，降低郵件身分偽冒風險，包含DNS認證、支援SPF/DKIM/DMARC、郵件標頭偽造偵測以及郵件詐騙或商業詐騙偵測機制、智慧偵測相似網域詐騙風險，協助機關同仁第一時間避開偽冒信件風險。 |
| 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)  Openfind網擎資訊雲端服務資料識別採取 user level / domain level / system level 透過權限控管帳號可使用範圍 |
| 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)  Openfind網擎資訊雲端服務提供外寄安全服務，針對重要的資料，可提供外寄加密的服務，妥善保護溝通資訊；另外在檔案分享方面，也規劃了檔案存取權限控制的機制，帳號只能依照被賦予的權限進行檔案存取。 |
| 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)  Openfind網擎資訊雲端服務提供郵件稽核服務，能有效降低內寄外信件不慎外寄重要機關文件、或異常個資外洩的狀況。 |
| 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)  Openfind網擎資訊雲端服務遵循 ISO27001條文 A.8.13 資訊備份、A.8.14 資訊處理設施之多重備援、A.8.16 監視活動等要求，對於虛擬主機映像檔定期進行備份與監控管理。 |
| 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)  Openfind網擎資訊雲端服務提供多因子認證方式登入，用戶可依據需求以 OTP 方式登入服務，以確保帳號安全。 |
| 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)  Openfind網擎資訊雲端服務符合零信任精神，在身分鑑別/設備鑑別/信任推斷等項目，可配合機關實現零信任相關規範，並提供多面向管理報表，方便資訊管理者查閱監控，提升資安管理效能。 |