**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**

雲端平台(PaaS或IaaS)共通性資通安全基本要求

|  |  |
| --- | --- |
| 雲端服務名稱 | CW MDM KC CLOUD |
| 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 19 日 |
| **高** | **中** | **普** |
| 提供平台服務商 | 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)。 |
| 廠商不得為大陸地區廠商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」。 |
| 弱點管理 | 雲端應用系統平台具備定期檢視PaaS 之應用、組件或 Web 服務是否存在漏洞並進行更新修補 | ● | ● | ● | 我司雲端服務使用AWS EC2服務，其中包含Amazon In-spector ，一項自動化漏洞管理服務，可不斷掃描 Amazon Elastic Compute Cloud (EC2)、AWS Lambda 函數，以及 Am-azon ECR 中和持續整合與持續交付 (CI/CD) 工具內的容器映像，以即時尋找軟體漏洞和意外網路風險。 |
| 存取控制 | 雲端應用系統平台提供帳號安全認證、權限管理、網路安全傳輸及遠端存取控管佐證 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列具體說明) 1. 雲端服務帳號權限管理機制。  2. 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。 |
| 須針對維運管道建立基於零信任(ZTA)控管基礎之防護機制，並導入同等(AAL2)或更高等級的多因子身份鑑別機制 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列具體說明說明雲端服務之零信任防護與多因子認證機制) |
| 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)**        1. 登入日誌(logon log)**(必要)**      1. 網站日誌(web log)**(必要)**      1. 作業系統日誌(OS event log)：     系統有報錯的話，上圖會記錄，我司所使用之AWS EC2也有紀錄log的服務。  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)。 |
| 營運持續計畫 | 檢視廠商平台營運持續、資料復原計畫及執行情形 | ● | ● | ● | 我司根據ISO 27001:2022規範，已建立、實施並持續維護營運持續計畫及資料復原計畫。 |
| 變更管理/安全管理 | 雲端應用系統平台具備變更管理制度 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列具體說明雲端服務變更管理制度做法) |
| 雲端應用系統平台具備設定安全管理制度 | ● | ● | ● | 我司根據ISO 27001:2022規範，已建立、實施雲端應用系統平台安全管理制度。 |
| 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。 |
| 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。 |
| 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) |
| 雲端應用系統平台內如存有機密或個人資料應依相關法令強化資料安全防護措施 | ● | ● | ● | 我司根據ISO 27001:2022規範，已依相關法令強化服務機密或個人資料資料安全。 |
| 資安防護建置持續監控 | 資安監控(SOC)機制，廠商須提供 7x24 小時全天候監控 | ▲ | ▲ | ▲ | (為訂購機關資通安全責任等級辦理時參考，廠商自行選擇是否填寫) |
| 須提供資安事件應變服務(Emergency Response Service) | ▲ | ▲ | ▲ | (為訂購機關資通安全責任等級辦理時參考，廠商自行選擇是否填寫) |
| 具備相關網路入侵防護、實體入侵防護、監測活動管理或防毒機制(DDoS 防護服務、防毒、防火牆、IPS/IDS、WAF、APT等) | ▲ | ▲ | ▲ | (為訂購機關資通安全責任等級辦理時參考，廠商自行選擇是否填寫) |
| 導入端點偵測與回應機制(Endpoint Detection and Respons, EDR) | ▲ | ▲ | ▲ | (為訂購機關資通安全責任等級辦理時參考，廠商自行選擇是否填寫) |
| 導入VANS (Vulnerability Alert and Notification System, VANS) | ▲ | ▲ | ▲ | (為訂購機關資通安全責任等級辦理時參考，廠商自行選擇是否填寫) |
| 導入GCB(Government Configuration Baseline) | ▲ | ▲ | ▲ | (為訂購機關資通安全責任等級辦理時參考，廠商自行選擇是否填寫)  如有不適用規則，應擬具管理或替代作為，並提請機關資安長確認風險。 |
| 資安演練 | DDoS (Distributed Denial of Service)攻防演練 | ◎ | ◎ | ◎ | (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) |
| 入侵與攻擊模擬 (Breach and Attack Simulation)演練  (涉及重要對外服務之系統建議評估辦理) | ◎ | ◎ | ◎ | (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) |
| 紅藍隊演練  (涉及重要對外服務之系統建議評估辦理) | ◎ | ◎ | ◎ |
| 資安檢測 | 主機弱點掃描 | ● | ● | ● | 雲端服務定期進行主機弱點掃描及網站弱點掃描。 |
| 網站弱點掃描 | ● | ● | ● |
| 滲透測試掃描(由檢測人員測試雲端服務是否具備TLS v1.2以上安全通訊協定) | ● | ◎ | ◎ |
| 雲端服務之APP取得行動應用 App 基本資安標章或其他具有同等級認證 | ● | ● | ◎ | □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 |
| 資安健診 | ● | ● | ● | ■依委託機關需求執行資安檢測  ■依機關規劃另案配合執行 |