**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**

雲端平台(PaaS或IaaS)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：　　eDC Cloud

**☑**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 11 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：**  本公司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 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.雲端安全聯盟CSA Star。   1. 4.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. 本公司為宏碁股份有限公司投資之子公司，非「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」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 | ● | ● | ● | 針對雲端服務平台(CSP)每季定期執行網頁弱掃，如有弱點，於當季修補完成後進行覆測。 |
| 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 | ● | ● | ◎ | 雲端服務管理平台CSP，需經由VPN連線至本公司網段才能存取相關資源，且帳號具備權限功能，僅開通的服務可供存取。 |
| 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 | ● | ● | ◎ | 雲端服務平台CSP具備零信任控管機制，除了使用VPN連線後，才能看到登入頁面，當輸入帳號密碼後，會寄出一個連結到他個人信箱，透過此連結，才能登入CSP平台。 |
| 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 | ● | ● | ● | **本公司採用自行研發的日誌保存系統SAFE3.0保存雲端服務系統日誌至少6個月，保存項目包括：**   1. 應用程式日誌(AP log) 2. 登入日誌(logon log) 3. 網站日誌(web log) 4. 作業系統日誌(OS event log)   補充說明: 定底層主機設定拋送Log至日誌保存系統(safe3.0)後，即可在safe3的portal查詢，如附件名稱:safe3 Portal查詢結果.png |
| 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 | ● | ● | ● | 於ISO27001標準中訂定「服務中斷回復程序書」及「事故管理程序書」，說明事件復原處理程序。  請參考附件： |
| 變更管理/安全管理 | 雲端應用系統平台具備變更管理制度 | ● | ● | ◎ | 本公司之雲端服務通過 ISO20000驗證，所有變更均依變更管理制度進行，於系統中申請變更，經核准後執行。 |
| 雲端應用系統平台具備設定安全管理制度 | ● | ● | ● | 本公司通過ISO27001驗證，安全管理訂定於「系統維運安全程序書」中。  請參考附件： |
| 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：**  本公司雲端服務機房設置於桃龍潭，備援至台北內湖，無國外機房，因此無資料移轉至本國以外問題。 |
| 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：**  本公司雲端服務機房設置於桃園龍潭，備援至台北內湖，無傳輸於大陸地區(含香港及澳門地區)情況。 |
| 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 | ● | ● | ◎ | 對於虛擬主機映像檔，每天使用備份工具備份至其他儲存設備(NAS)存放。 |
| 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 | ● | ● | ● | 本公司通過ISO27018規範，針對保護個人識別資訊，均依標準規定辦理。 |
| 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 | ▲ | ▲ | ▲ | eDC雲端對外服務之防火牆及重要閘道端設備，委由安碁資訊進行7x24 SOC監控服務。 |
| 須提供資安事件應變服務(Emergency Response Service) | ▲ | ▲ | ▲ | 無 |
| 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) | ▲ | ▲ | ▲ | 需選購相關服務後進行部署。 |
| 導入端點偵測與回應機制(Endpoint Detection and Respons, EDR) | ▲ | ▲ | ▲ | 無 |
| 導入VANS (Vulnerability Alert and Notification System, VANS) | ▲ | ▲ | ▲ | 無 |
| 導入GCB(Government Configuration Baseline) | ▲ | ▲ | ▲ | 無 |
| 資安演練 | DDoS (Distributed Denial of Service)攻防演練 | ◎ | ◎ | ◎ | 無 |
| 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) | ◎ | ◎ | ◎ | 選購後以專案方式提供服務。 |
| 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 | ● | ● | ● | 網站弱點掃描及滲透測試每年委外由安碁資訊進行檢測。每季進行網頁弱掃一次（含修補後之覆測）。每年進行一次滲透測試（含修補後之覆測）。 |
| 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 | ● | ● | ● | 可配合 |