**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：　雲端虛擬資源(IaaS)

⬛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 月 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 | ● | ● | ● | 本平台依據國際標準ISO27001，為確保資訊安全，制定並實施了定期的漏洞檢視程序。每年，依據該標準進行全面的漏洞評估，以辨識系統中的潛在風險。根據檢視結果，針對中高風險及以上等級的漏洞，進行及時修復和改進，從而有效地降低資訊安全風險，保護平台及用戶的數據安全。  上列資安檢測報告已經於今年ISO27001換證時,由第三方驗證機構驗證過,但由於報告中含有機密資料,無法截圖提供,但可以至本司查核相關報告 |
| 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 | ● | ● | ◎ | 1. 本雲端服務帳號具備權限管理機制，可依據權責區分。 2. 本雲端服務具備「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 | ● | ● | ◎ | 支援MFA機制,可配合機關需求提供2FA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 | ● | ● | ● | **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)：   上述1~4項都能執行保存  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 | ● | ● | ● | 本平台服務依據ISO 27001，有訂定營運持續、資料復原計畫,並定期執行相關演練。  數位通 雲端營運持續 , 按程序 已於 2023/5/23 執行演練完成並已產出報告  ISMS-L3-20-F01-230523-01  上列報告已經於今年ISO27001換證時,由第三方驗證機構驗證過,但由於報告中含有機密資料,無法截圖提供,但可以至本司查核相關報告 |
| 變更管理/安全管理 | 雲端應用系統平台具備變更管理制度 | ● | ● | ◎ | 本平台服務依據ISO 27001，具備管理制度變更。  具體而言，我們設有主管理者、次管理者及一般使用者三種角色，以便根據不同的管理需求和權限範圍進行分級管理。主管理者負責系統的全盤管理與重大變更，次管理者協助執行變更並監控日常操作，一般使用者則僅限於進行基礎操作和使用功能，從而確保變更過程的安全性與系統運作的穩定性。 |
| 雲端應用系統平台具備設定安全管理制度 | ● | ● | ● | 本平台服務依據ISO 27001，具備設定安全管理制度。 |
| 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：**  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 | ● | ● | ◎ | 雲端平台用戶可以需求上傳映像檔，但上傳的檔案僅有該用戶能夠取用，其他平台用戶無法讀取及使用 |
| 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 | ● | ● | ● | 依據ISO 27017及ISO 27018相關規範及程序，來執行並強化資料安全防護措施  也有完善的安全管理制度，以確保資訊安全和系統穩定性。根據該制度，僅有經過授權且具備相關權限的帳號才能執行安全管理操作。這些操作包括但不限於安全設定、權限調整、系統監控及風險評估等。通過這一措施，我們確保只有經過適當授權的專業人員才能對系統進行關鍵的安全配置與管理，從而有效防範潛在的安全威脅，維護平台的整體安全性。 |
| 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 | ▲ | ▲ | ▲ | 有提供資安監控(SOC)機制之加值服務 , 可依機關規劃另案配合執行。 |
| 須提供資安事件應變服務(Emergency Response Service) | ▲ | ▲ | ▲ | 有提供資安事件應變服務(Emergency Response Service)之加值服務 , 可依機關規劃另案配合執行。 |
| 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) | ▲ | ▲ | ▲ | 有提供網路入侵防護、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)加值服務 , 可依機關規劃另案配合執行。 |
| 導入端點偵測與回應機制(Endpoint Detection and Respons, EDR) | ▲ | ▲ | ▲ | 有提供端點偵測與回應機制(Endpoint Detection and Respons, EDR)加值服務, 可依機關規劃另案配合執行。 |
| 導入VANS (Vulnerability Alert and Notification System, VANS) | ▲ | ▲ | ▲ | 有提供端點偵測與回應機制(Endpoint Detection and Respons, EDR)加值服務, 可依機關規劃另案配合執行。 |
| 導入GCB(Government Configuration Baseline) | ▲ | ▲ | ▲ | 有提供端點偵測與回應機制(Endpoint Detection and Respons, EDR)加值服務 , 可依機關規劃另案配合執行。 |
| 資安演練 | DDoS (Distributed Denial of Service)攻防演練 | ◎ | ◎ | ◎ | 有提供DDoS (Distributed Denial of Service)攻防演練加值服務 , 可依機關規劃另案配合執行。 |
| 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) | ◎ | ◎ | ◎ | 有提供入侵與攻擊模擬演練、紅藍隊演練的加值服務 , 可依機關規劃另案配合執行。 |
| 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 | ● | ● | ● | 依規定定期執行系統弱點掃描、網站弱點掃描及滲透測試掃描  有提供左列各項資安檢測服務，可依機關規劃另案配合執行。 |
| 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 | ● | ● | ◎ | 本雲端服務不提供App，因此不適用此要求 |
| 資安健診 | ● | ● | ● | 有提供資安健診服務，可依機關規劃另案配合執行。 |