**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：台智雲 -雲端服務

⬜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 10 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：**  所提供雲端服務皆為驗證範圍內，本公司擁有ISO　27001有效證書(證書編號[TW22/00056](https://www.sgsgroup.cz/en/vr/certified-client-directory))，雲端服務則以原廠合作之公有雲業者通過驗證證書代之，國網中心通過ISO　27001、ISO　27017、ISO 27018，可參照國網官網[認證網站](https://www.nchc.org.tw/Page?itemid=101&mid=171)說明。 |
| 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：**  台灣智慧雲端服務股份有限公司，統一編號：91120763，本公司為100%台灣本土企業，可查詢經濟部商業發展署 [商工登記公示資料查詢服務網站](https://findbiz.nat.gov.tw/fts/query/QueryBar/queryInit.do?disj=E8EE52E0EA524923FE6AEA9040A8DDB5&fhl=zh_TW)。 |
| 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 | ● | ● | ● | 全平台定期進行SecurityScorecard(SSC)非侵入式掃描，依產製報告風險等級，通報平台維運單位及外部用戶進行安全性修補． |
| 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 | ● | ● | ◎ | 提供多租戶設計並提供角色與權限管理機制，詳細請參閱官網  「[角色總覽及權限比較](https://docs.twcc.ai/docs/concepts-tutorials/tws-member-center/concepts/role-overview/)」說明文件，雲端服務均支援TLS(Transport Layer Security)v1.3版本的安全通訊網路傳輸協定，並經[Qualys SSL Labs驗證](https://www.ssllabs.com/ssltest/)，檢驗為『A+』等級。 |
| 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 | ● | ● | ◎ | 雲端服務登入頁面採用雙因子認證 (MFA) 功能，登入時需再輸入OTP驗證碼進行第二階段驗證．以強化帳戶安全性。HPC驗證碼則導入全景軟體「[IDExpert](https://www.changingtec.com/idexpert.html)」符合零信任(ZTA)控管要求 |
| 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，參閱雲端服務[操作手冊](https://docs.twcc.ai/docs/user-guides/twcc/general/activity-history/)平台相關工作日誌，檢視服務使用歷史紀錄，用戶可以雲端服務網站、CLI 使用的服務功能，這兩種操作皆是透過呼叫API 以完成各項作業，而服務操作的歷史紀錄可透過使用者網站檢視，並下載紀錄檔案，可以從記錄判斷：啟動作業的成員，啟動作業的方法 (GET/PUT/PATCH/POST/DELETE)，對哪些服務進行操作  作業的狀態，請求時間，來源位址，而用戶容器服務及虛擬主機作業系統日誌(OS event log)，應用程式日誌(AP log)、登入日誌(logon log)、網站日誌(web log)、作業系統日誌(OS event log)建議外抛至[COS雲端物件儲存空間](https://tws.twcc.ai/service/cloud-object-service/)，本項用戶日誌保存將由客戶人員協助專業服務，以滿足日誌項目保存期限：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 | ● | ● | ● | 依據ISO27001標準的要求，參照營運持續管理規範(文件編號SR-013)定期執行演練，且持續確保ISO 27001證書有效。 |
| 變更管理/安全管理 | 雲端應用系統平台具備變更管理制度 | ● | ● | ◎ | 參照ITCM流程說明文件( <https://tinyurl.com/2yhfv99z> )。 |
| 雲端應用系統平台具備設定安全管理制度 | ● | ● | ● | 變更管理皆需於變更前及變更後，皆需通過Cyber Security Check、風險評估，如務中斷或元件重啟，可能造成用戶資料遺失，根據變更風險 ，依「重要度」，「影響程度」及「風險性」進行不同等級的處置，如離峰時間變更，由自動變更改為人工變等等。 |
| 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：**  本公司所營運雲服務係建構於國家高速網路與計算中心的國家級 AI 研發與雲端服務基礎設施，主資料中心坐落於台中分部，並以台南分部作為備援資料中心。各資料中心地址如下：國網中心臺中分部：40763 臺中市西屯區科園路22號；國網中心臺南分部：74147 臺南市新市區南科三路28號。 |
| 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：**  不適用，如上題所述，無其它跨境機房。 |
| 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 | ● | ● | ◎ | 雲服務平台已啟動openstack[映像檔加密機制](https://tinyurl.com/28f4p97w)，用戶可參照使用手冊[磁碟加密](https://docs.twcc.ai/docs/user-guides/twcc/vcs/vds/create-encrypted-data-disks/)專章自行選用。 |
| 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 | ● | ● | ● | 雲端服務通過ISO 27018:2019個人隱私資料保護，定期由獨立第三方評估機構驗證，以協助用戶於雲端服務環境建立安全可控的作業環境。 |
| 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 | ▲ | ▲ | ▲ | 已加入TWCERT/CC台灣電腦網路危機處理暨協調中心，並設有資訊安全維運中心，透過網路型入侵偵測防禦系統（Network Intrusion Prevention System），監控網路流量，偵測異常行為並即時阻絕網路攻擊，並針對威脅行為進行告警與資安事件通報應變處置，以確保網路服務主機安全。 |
| 須提供資安事件應變服務(Emergency Response Service) | ▲ | ▲ | ▲ | 參照官網揭露隱[私權及資訊安全政策及資通安全事件通報機制](https://tws.twcc.ai/privacy/)，資安事件應變電子郵件：security@twsc.io。 |
| 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) | ▲ | ▲ | ▲ | 參照官網[資安防護服務](https://tws.twcc.ai/cloud-security/)專章說明。 |
| 導入端點偵測與回應機制(Endpoint Detection and Respons, EDR) | ▲ | ▲ | ▲ | 依不同作業系統，採取不同方案，微軟 Windows建議啟動 defender自動掃描 ，Linux作業建議[ClamAV](https://www.clamav.net/)防毒軟體或[OpenVAS](https://www.openvas.org/)做系統弱點掃描。 |
| 導入VANS (Vulnerability Alert and Notification System, VANS) | ▲ | ▲ | ▲ | 資安弱點通報機制(VANS)應導入範圍為全平台，除定期進行SecurityScorecard(SSC)非侵入式掃描，依資通情資來源及Palo Alto Networks防火牆偵測中高風險異常行為，通報用戶及上級指導單位。 |
| 導入GCB(Government Configuration Baseline) | ▲ | ▲ | ▲ | 提供7 ×24 客服中心，可協助用戶依據政府組態基準（GCB）進行相關設定。 |
| 資安演練 | DDoS (Distributed Denial of Service)攻防演練 | ◎ | ◎ | ◎ |  |
| 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) | ◎ | ◎ | ◎ |  |
| 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 | ● | ● | ● | 可建議掃描工具供用戶進行資安檢測，本公司每季會針對內部系統進行弱點掃描，核心系統均配合維運專案，每季進行主機弱點掃描，掃描結果無低、中、高資安風險，客戶服務系統屬公司內部系統，已進行網路阻隔，無公共網路暴露風險，雲端服務均支援TLS(Transport Layer Security)v1.3版本的安全通訊網路傳輸協定，並經[Qualys SSL Labs驗證](https://www.ssllabs.com/ssltest/)，檢驗為『A+』等級。 |
| 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。  **本題不適用，無提供行動應用App服務** |
| 資安健診 | ● | ● | ● | 1. 為符合政府網站服務管理規範，將由原廠合作之公有雲業者(國網中心)，每年至少一次委由民間資安專業公司，定期執行全平台資安健診，依據健檢報告指引，採取適當防護措施、排除潛在的威脅。  2. 用戶於使用雲端服務期間，本團隊可配合用戶指定範圍辧理資安檢測，以確保使用者可以安心使用雲端服務。 |