**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：　hicloud雲端虛擬服務 / hicloud 雲端加值服務 / hicloud 主權雲服務

█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 4 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：**  中華電信遵循行政院院臺護長字第1090201804A 號函之要求事項，公司採購之資通訊設備，皆需符合「資通信資訊設備請購資安審查檢核表」要求，已限制採購設備不得為中國大陸地區品牌、非中國大陸地區製造及非陸資投資之廠商。 |
| 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 | ● | ● | ● | 依據中華電信資通安全處及各原廠(VMware、Cisco、Juniper、HP、Dell…)等公告進行漏洞更新修補。 |
| 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 | ● | ● | ◎ | 1. hicloud雲端平台機關填寫hicloud服務申請書並用印後，會進行審核及帳號開通第一個管理者帳號。登入後可透過IAM(子帳號功能)根據需求，開通不同權限子帳號。      2. hicloud傳輸採https方式加密，並使用TLSv1.2通訊協定。 |
| 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 | ● | ● | ◎ | hicloud登入須提供「帳號」+「密碼」+「圖形驗證碼」+「OTP」提供多因子身份鑑別制 |
| 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)：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)。   1. hicloud雲端平台提供日誌功能，日誌最長保留12個月。 2. 日誌記錄雲端平台包含AP log、logon log、web log等，關於虛擬機操作、資源申退租、資源變更、使用者及IAM子帳戶登入登出記錄、防火牆異動。 3. hicloud提供IaaS服務為主，OS層以內的資料須由用戶登入OS後自行操作管理，故無法直接提供此項日誌內容。但用戶登入後，可自行設定OS log轉拋到其他syslog server進行保存，以滿足6個月保存需求。 |
| 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 | ● | ● | ● | 為確保hicloud雲端平台營運持續，每年執行二次BCP持續營運演練，以符合ISO 27001、27017、27018及CSA STAR要求。 |
| 變更管理/安全管理 | 雲端應用系統平台具備變更管理制度 | ● | ● | ◎ | hicloud雲端平台提供用自行操作管理雲端資源變更，包括雲端平台申租、網路頻寬、VM主機規格、儲存、備份計畫、負載平衡、資安服務(IPS、DDoS、WAF)等需求，皆可透過雲端平台自行操作變更。 |
| 雲端應用系統平台具備設定安全管理制度 | ● | ● | ● | hicloud雲端平台從用戶登入開始，執行雲端平台操作皆可透過log進行查詢。服務設定皆會透過UI提示用戶進行確認後，系統才會進行設定，以避免用戶誤操作。 |
| 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。  hicloud雲端服務主機與雲端服務系統系統平台皆建置於中華電信雲端機房，雲端資料儲存地皆在我國境內。hicloud資訊安全暨隱私權政策請參考以下網址：https://cloud.hinet.net/assets/hicloud/security\_announce.pdf |
| 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。  hicloud雲端服務主機與雲端服務系統系統平台皆建置於中華電信雲端機房，雲端資料儲存地皆在我國境內。hicloud資訊安全暨隱私權政策請參考以下網址：https://cloud.hinet.net/assets/hicloud/security\_announce.pdf |
| 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 | ● | ● | ◎ | hicloud通過ISO 27001、ISO 27017、ISO 27018及CSA STAR Level 2驗證，並取得相關證書，確保雲端平台架構安全。  hicloud虛擬主機平台皆存放在維運網路內，透過網路VLAN技術區隔維運網路及儲存區網路，儲存網路為獨立隔離網段無法直接存取。維運人員操作維運終端皆要求安裝Trend Micro Apex One Security Agent、iServer Agent及Syslog轉拋工具，以確保維運終端資安，定期監控防毒碼更新、系統Patch更新、操作行為監控及日誌轉拋SOC統一監控。  1. 維運終端安裝防毒軟體    2. 維運終端安裝中華自主研發資安管理系統     1. 維運終端日誌轉拋SOC監控服務 |
| 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 | ● | ● | ● | 客戶資料運用方式/衍生資料/衍生資料使用範圍/衍生資料存取權限，依中華電信股份有限公司個人資料保護暨蒐集告知條款辦理，本公司依「個人資料保護法」相關規定，蒐集、處理及利用您於本網站登錄、留存之個人資料，並妥善加以保管。非經客戶的同意或依法令之規定，本公司絕不對外揭露。 |
| 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 | ▲ | ▲ | ▲ | 可整合中華資安服務提供服務 |
| 須提供資安事件應變服務(Emergency Response Service) | ▲ | ▲ | ▲ | 可整合中華資安服務提供服務 |
| 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) | ▲ | ▲ | ▲ | 可整合中華資安服務提供服務 |
| 導入端點偵測與回應機制(Endpoint Detection and Respons, EDR) | ▲ | ▲ | ▲ | 可整合中華資安服務提供服務 |
| 導入VANS (Vulnerability Alert and Notification System, VANS) | ▲ | ▲ | ▲ | 可整合中華資安服務提供服務 |
| 導入GCB(Government Configuration Baseline) | ▲ | ▲ | ▲ | GCB須登入OS佈署及調整，建議由用戶或授權委外廠商處理。 |
| 資安演練 | DDoS (Distributed Denial of Service)攻防演練 | ◎ | ◎ | ◎ | 可整合中華資安服務提供服務 |
| 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) | ◎ | ◎ | ◎ | 可整合中華資安服務提供服務 |
| 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 | ● | ● | ● | 可整合中華資安服務提供服務 |
| 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 | ● | ● | ● | 可整合中華資安服務提供服務 |