衛生福利部主權雲服務指南

Guideline for Sovereign Cloud Services

Ministry of Health and Welfare

壹、總則

一、訂定目的

衛生福利部（以下簡稱本部）及所屬機關（構）為確保國家醫療健康大數據、個人資料及國家關鍵基礎設施（CI）資通系統在導入雲端化過程中，具備技術自主性、資料安全性與法律管轄權，特訂定本指南。

二、核心價值

本指南旨在落實「數位主權」核心價值，規範國內外公有雲服務供應商（以下簡稱供應商）於技術、人員、法律及營運四大維度之合規標準，以符合資通安全管理法及相關委外辦理資通業務之法規要求。

三、適用範圍

本部及所屬機關（構）使用雲端服務執行業務或提供公眾服務者，均適用本指南。後續將視國內機制成熟度及全球技術趨勢，採滾動式修正。

貳、八大核心技術方針

供應商除應通過 ISO/IEC 27001（資訊安全管理）、ISO/IEC 27017（雲端服務安全）及 ISO/IEC 27018（雲端個資保護）相關國際認證外，須符合下列技術指標：

一、全程加密與金鑰自主（Encryption & Key Autonomy）

(一)靜態資料（At-rest）：儲存資料必須採用不低於 AES-256 之強健加密演算法。

(二)傳輸資料（In-transit）：強制採用 TLS 1.2 以上協定，禁用具已知弱點之密碼組（Cipher Suites），並支援完美前向安全性（PFS）。

(三)演算法等級：非對稱加密應採用 RSA-3072 或 ECDSA P-384 以上等級，並應支援密碼敏捷性(Cryptographic Agility)架構，以利未來銜接次世代加密標準(含後量子密碼學 PQC)。

(四)管理模式：必須支援「客戶自管金鑰（CMK）」或「自持金鑰（HYOK）」模式。本部須具備金鑰唯一控制權，供應商未經授權不得解密任何資料。(本條技術規格定位為高安全等級套餐服務，由各機關及醫療院所依業務需求及預算規劃，採分階段方式自主導入)

二、資料二次利用授權規範（Secondary Use Authorization）

未經本部書面授權，供應商不得將本部資料（含原始資料、中繼資料 Metadata 及日誌資料 Log）用於人工智慧訓練、模型優化、商業分析或任何非契約約定之目的。

三、不可逆之刪除協議（Irreversible Deletion）

服務終止時，供應商須執行加密抹除（Crypto-erasure），確保所有儲存層級之資料殘餘及備份皆無法還原，並提交具法律效力之物理或數位銷毀證明。

四、資料在地化（Data Residency）

本部工作資料、中繼資料、備份及備援資料，其物理存放位置必須位於我國境內之資料中心。

五、維運人員國籍管制（Personnel Nationality Control）

(一)具備高權限之系統管理員及相關業務主管，不得為具備大陸地區、香港或澳門國籍之人員。

(二)供應商應以技術管控措施(含客戶自管金鑰 CMK/HYOK)及通過 ISO 27001、SOC 2 相關國際資安認證，作為確保人員無預設資料存取權限之合規證明。

六、數位韌性與雙活架構（Cyber Resilience & Dual-Active）

(一)架構要求：針對關鍵系統，供應商須提供我國境內「雙活（Dual-Active）」或「異地多可用區（Multi-AZ）」架構。

(二)效能指標：復原點目標（RPO）應趨近於零，復原時間目標（RTO）應達成最小化，確保災變時醫療體系運作不中斷。

七、法律優先與管轄權（Legal Primacy）

(一)服務應遵循資通安全管理法及個人資料保護法規定。

(二)契約爭議管轄法院應為我國法院。若外國法律與我國法律衝突，應以我國法律為最優先準則。

八、透明化稽核與監控（Auditing & Monitoring）

(一)供應商應賦予本部「稽核權」及「實體機房稽核權」。

(二)管理員操作日誌（Admin Audit Logs）須即時存檔，或依要求串流至本部指定之資安監控中心（SOC）。

參、關鍵增補規範（Sovereignty Enhancements）

一、技術支援主權（Sovereignty of Support）

涉及資料存取之技術支援或遠端排障之境內團隊成員(含分包廠商)，不得由具備大陸地區、香港或澳門國籍之人員執行。境外團隊成員執行涉及本部資料之技術支援時，至少應具備相關國際資安標準(含 ISO 27001 或 SOC 2)所定之人員安全管控機制，並提供第三方驗證證明。嚴禁未經授權之遠端桌面共享；技術支援過程中，供應商應確保人員對客戶資料不具預設存取權限，相關存取授權應有時效限制且須留有完整稽核紀錄。

二、資料可攜性與退出策略（Exit Strategy）

(一)通用格式：供應商須支援非私有（Non-proprietary）之通用格式導出，確保資料可攜。

(二)無縫遷移：供應商須提交具體退出計畫，確保本部能於約定期限內完成業務無縫遷移。

三、對抗域外管轄權承諾（Anti-Extraterritoriality）

(一)通報義務：供應商遭遇外國政府（含依美國 CLOUD Act 或同性質域外管轄法律）之資料調取請求時，於法令許可之範圍內，應第一時間通報本部，不得故意延遲或隱匿。

(二)抵禦立場：除經我國法定程序核准外，供應商不得主動將本部資料交付予外國執法機關；供應商依所屬國家或地區強制性法令規定而被迫配合執法者，不在此限，惟仍應於法令許可下儘速通知本部。

(三)技術保護：供應商應提供客戶自管金鑰(CMK)或自持金鑰(HYOK)相關技術控管機制，確保即使在技術層面收到資料請求，亦因金鑰由本部自主保管而無法完成解密，以技術手段作為抵禦域外管轄之根本防線。

四、供應鏈安全透明化（Supply Chain Integrity）

(一)風險控管：嚴禁使用危害國家資通安全產品相關廠商之硬體或軟體組件，確保供應鏈安全。

(二)SBOM 揭露：針對本部採購或委託開發之客製化軟體(含專案導入開發、系統整合加值開發及其他非標準化商業現成品)，供應商應依數位發展部資通安全署所定相關規範或指引，及行政院公共工程委員會契約範本提供軟體物料清單(Software Bill of Materials,SBOM)，揭露組件來源及版本資訊。標準化公有雲服務(含 IaaS、PaaS、SaaS 相關商業標準化品牌產品)，暫不適用本項 SBOM 揭露要求，待本部與數位發展部資通安全署就雲端服務適用範疇完成確認後，再行增補規範。