AI 算力平台用戶資料安全與保存聲明書

Platform Data Protection, Multi-Tenant Physical Isolation & Mandatory Sanitization Statement

服務平台	https://aipower.dginfra.gov.tw/	**文件編號**	AIPOWER-DSP-2026-V1.0
適用對象	平台進駐業者、申請機構及各租戶用戶	**發布維運**	AI 算力平台營運團隊

【重點一】個資妥善保存	**【重點二】獨立租戶與實體隔離**	**【重點三】使用期滿強制銷毀**
遵循我國《個資法》，全站導入 TLS 1.3 與 AES-256 高強度加密，落實最小化蒐集與零信任（Zero Trust）存取控管。	模型與訓練資料享有專屬 Project 獨立租戶邊界，GPU 算力與儲存採硬體級實體切分，保障智財權專屬與零交叉存取。	服務結束或租期屆滿即自動啟動 NIST SP 800-88 不可逆資料淨空銷毀程序，所有容器、暫存、快照全數清空，保證平台零留存。

壹、 聲明宗旨與法規遵循

為保障使用「AI 算力共享服務平台（https://aipower.dginfra.gov.tw/，以下簡稱本平台）」之各產官學研業者及專案單位（以下簡稱「用戶」）之數位資產安全、商業機密與個人隱私，本平台營運與維運團隊特發表本《用戶資料安全與保存聲明書》。

本平台恪遵《個人資料保護法》、《資通安全管理法》、國家資通安全防護規範及 ISO/IEC 27001 資訊安全管理標準，建置 Palo Alto / Fortinet 次世代防火牆（NGFW）、WAF、高防 DDoS 清洗與 7x24 SOC/NOC 監控，針對「用戶個人資料妥善防護」、「演算法模型與訓練資料之獨立實體隔離」及「服務結束後強制不可逆銷毀」提出具法定約束力之技術承諾。

貳、 業者個人資料之妥善保存與安全防護機制

本平台就用戶所提交之負責人、專案聯絡人及技術人員之個人資料（姓名、任職機構、電子郵件、電話等），實施下列最高規格保護措施：

- 合規法定目的與最小化原則： 僅限於身分驗證、運算配額管理、資安緊急通報與維運通訊使用。非經用戶明確書面授權或法令要求，絕不用於其他目的或移轉予第三方。
- 傳輸與靜態儲存全面加密： 全站網路傳輸強制導入 TLS 1.3 協定加密；身分資料庫與認證憑證全面採用 AES-256 演算法進行靜態加密，密鑰管理受硬體安全模組（HSM）防護。
- 零信任（Zero Trust）與最小權限： 嚴格角色基礎存取控制（RBAC）。內部工程師未經雙重簽核，無權調閱任何個人身分資料。
- 不可竄改之全生命週期稽核日誌： 所有帳號登入、資料調閱與權限異動行為均產生防竄改稽核日誌（Audit Logs），保存期限完全符合國家資通安全法規要求。

參、 業者資料（模型與訓練資料）之獨立租戶與實體隔離機制

用戶存放於本平台之核心數位資產（原始訓練集、特徵資料、模型權重檔、微調參數、推論代碼及產出成果），享有架構級獨立租戶與硬體隔離保護：

- **獨立多租戶與微邊界隔離（Project Isolation）：** 每一進駐業者獲配專屬虛擬私有運算專案環境（VPC / Dedicated Namespace）。網路拓撲採取「預設全拒絕（Deny-All Perimeter）」政策，阻斷不同租戶間網路封包穿透與橫向連線。
- **高階 GPU 算力硬體與記憶體實體隔離：** 針對 NVIDIA H100 / AMD MI300X 等高階 AI 節點，採用硬體級直通（GPU Passthrough）或硬體切分技術。用戶獨占所分配之 GPU 運算單元與顯存（HBM/VRAM），運算暫存於任務結束即刻清空，杜絕不同租戶間記憶體殘留或交叉存取。
- **底層儲存實體分立與磁區隔離：** 用戶之持續性儲存分配獨立之邏輯磁區（LUN），具備獨立存取權杖與加密金鑰，嚴格禁止共用儲存目錄或跨租戶掛載。
- **百分之百資料主權保證（Zero Model Training Policy）：** 所有資料與模型智慧財產權完全歸屬用戶。本維運團隊特此承諾：絕不檢視、複製用戶資料或模型，絕不將用戶資產用於任何基礎模型之訓練、微調或測試。

肆、 服務終止後之資料「強制完整刪除與不留存」保證

本平台建立嚴謹且具防禦性之「資料終身生命週期政策」，落實專案結束即刻清空之零留存原則：

- **租期屆滿強制自動觸發：** 當用戶運算合約期滿、額度用畢或用戶主動終止服務時，於寬限期（供備份下載）屆滿後，即刻自動鎖定並進入強制銷毀程序。
- **平台零殘留承諾（Zero Data Retention Guarantee）：** 銷毀範圍涵蓋資料庫、分散式儲存、臨時快取、**容器映像檔及系統備份快照**（Snapshots）。清除完成後，平台伺服器與備份媒體中絕不留存任何用戶資產複本。
- **出具資料銷毀與清除證明：** 依用戶內部資安治理或專案驗收稽核需求，本平台維運團隊得正式出具「資料安全清除與銷毀證明書（Certificate of Data Erasure）」，載明銷毀時間戳記與標準以供存查。