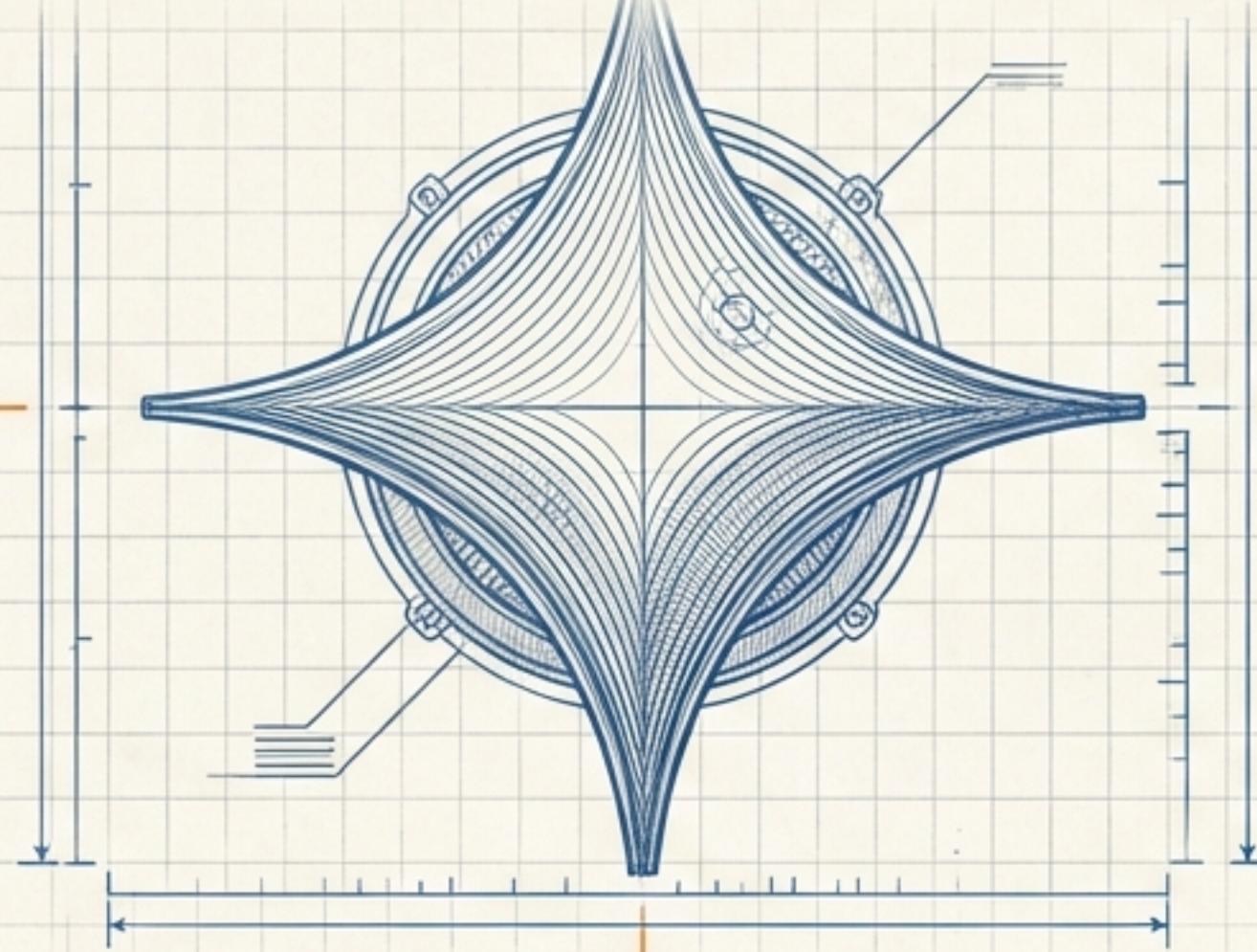


Google Cloud 生成式 AI 安全架構指南



保障您的數據擁有權、隱私與合規性

縱深防禦藍圖 v2025

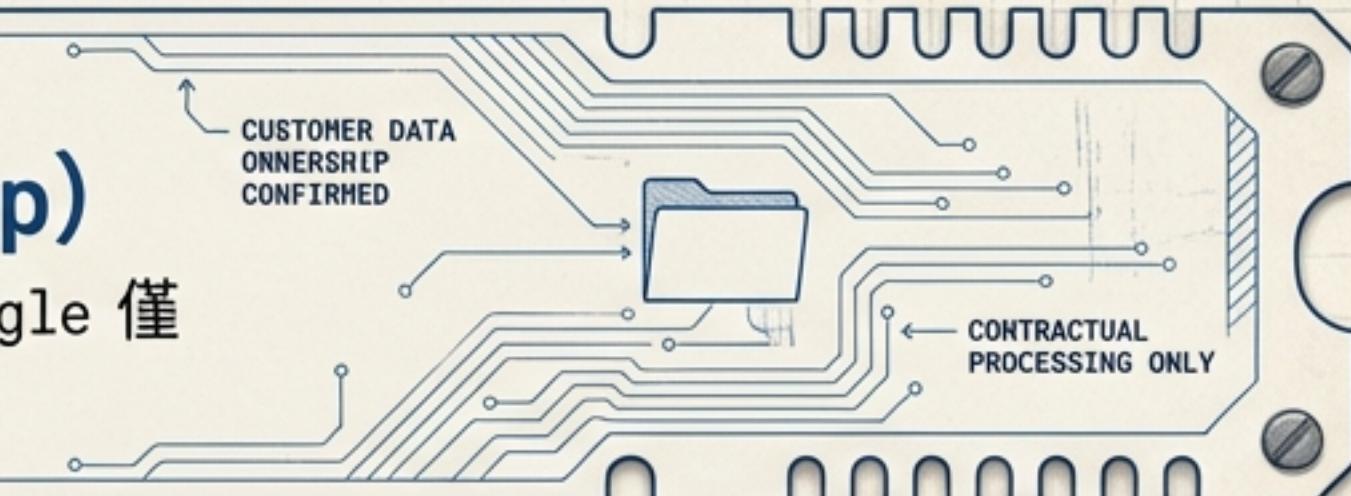
核心理念：數據歸您所有



System Rule No. 001

數據擁有權 (Data Ownership)

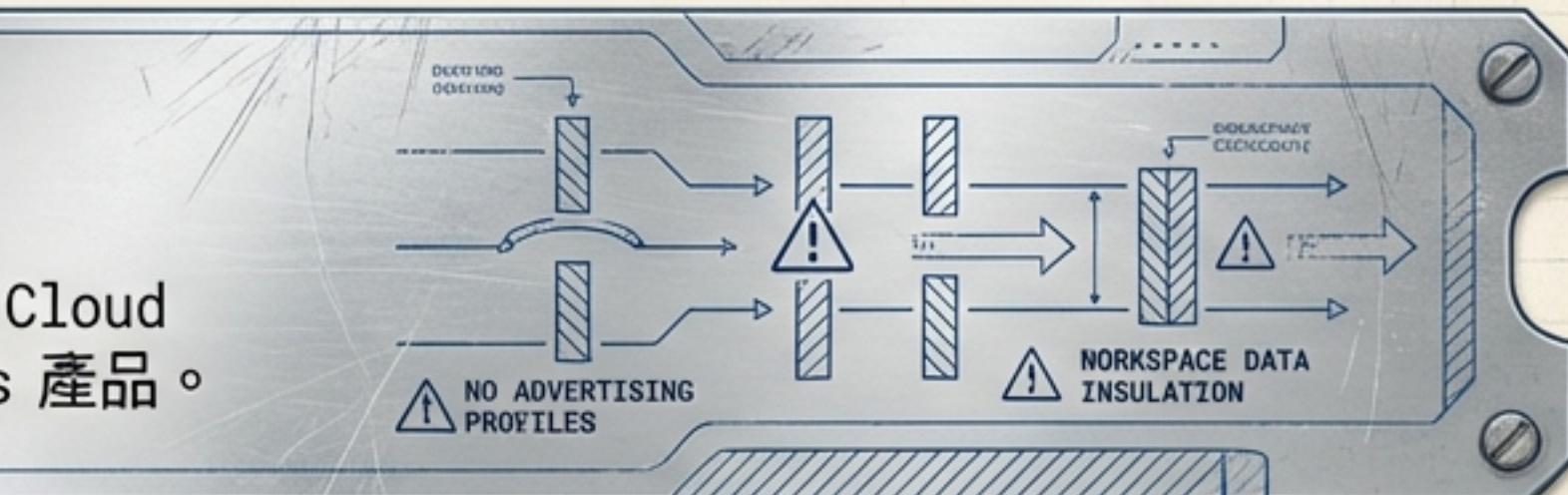
客戶數據完全屬於客戶，不屬於 Google。Google 僅依據合約協議處理數據，您隨時可刪除或匯出。



System Rule No. 002

絕不涉及廣告 (No Ads)

Google 絶不會使用您的 Workspace 或 Cloud 數據建立廣告設定檔或用於 Google Ads 產品。



System Rule No. 003

不販售數據 (No Selling)

Google 絶不會將客戶數據或服務數據販售給第三方。

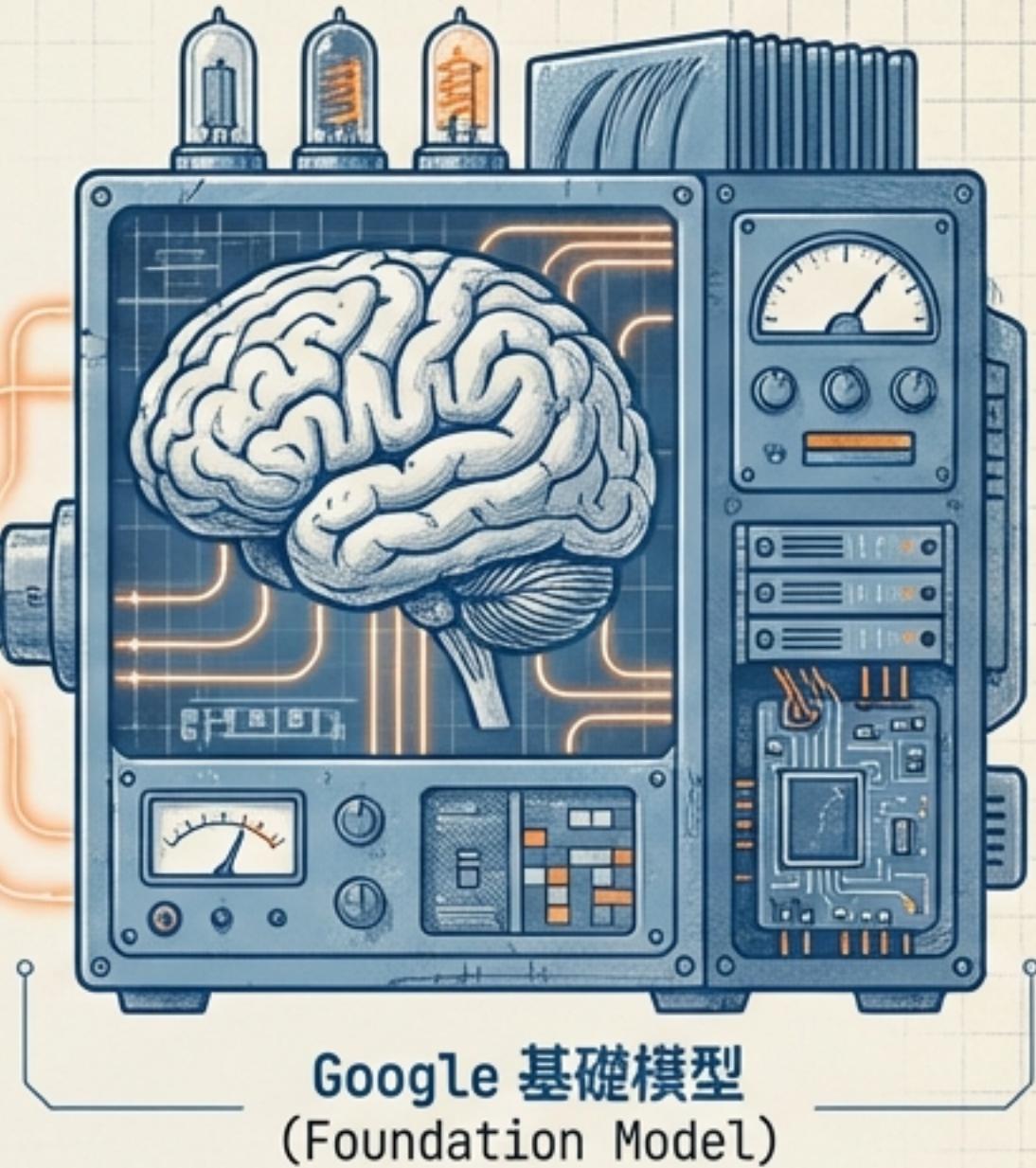


AI 訓練承諾：您的數據不會用於訓練基礎模型



未經許可，Google 不會使用您的 Workspace 數據來訓練或改進 Google 基礎的生成式 AI 模型（如 Gemini 或 Search）。

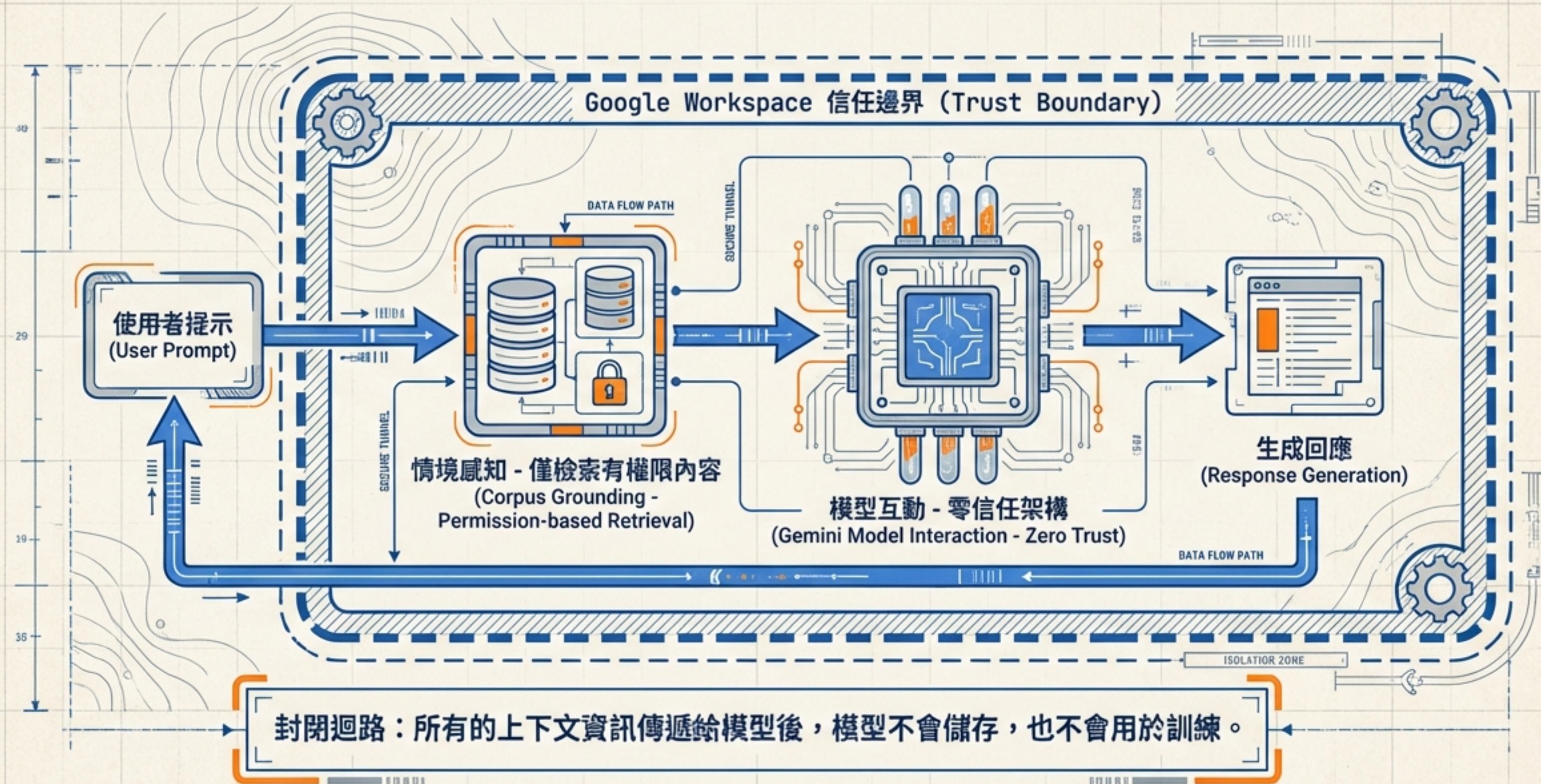
未經許可，Google 不會使用您的 Workspace 數據來訓練或改進 Google 基礎的生成式 AI 模型。



❖ **內容隔離**：您的提示（Prompts）和生成的內容不會與其他客戶共享。

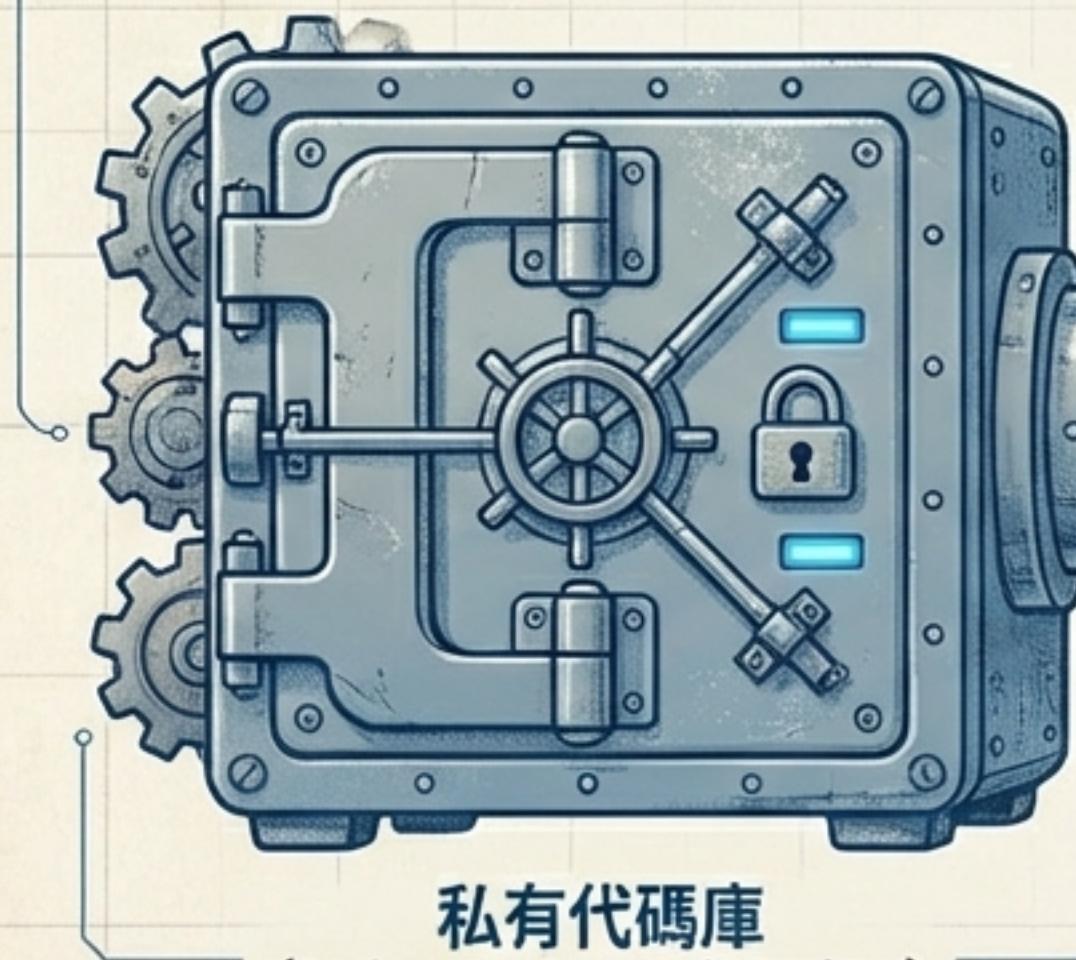
❖ **隱私設計**：您的數據不會被用於讓其他客戶受益。

信任邊界與資料流向



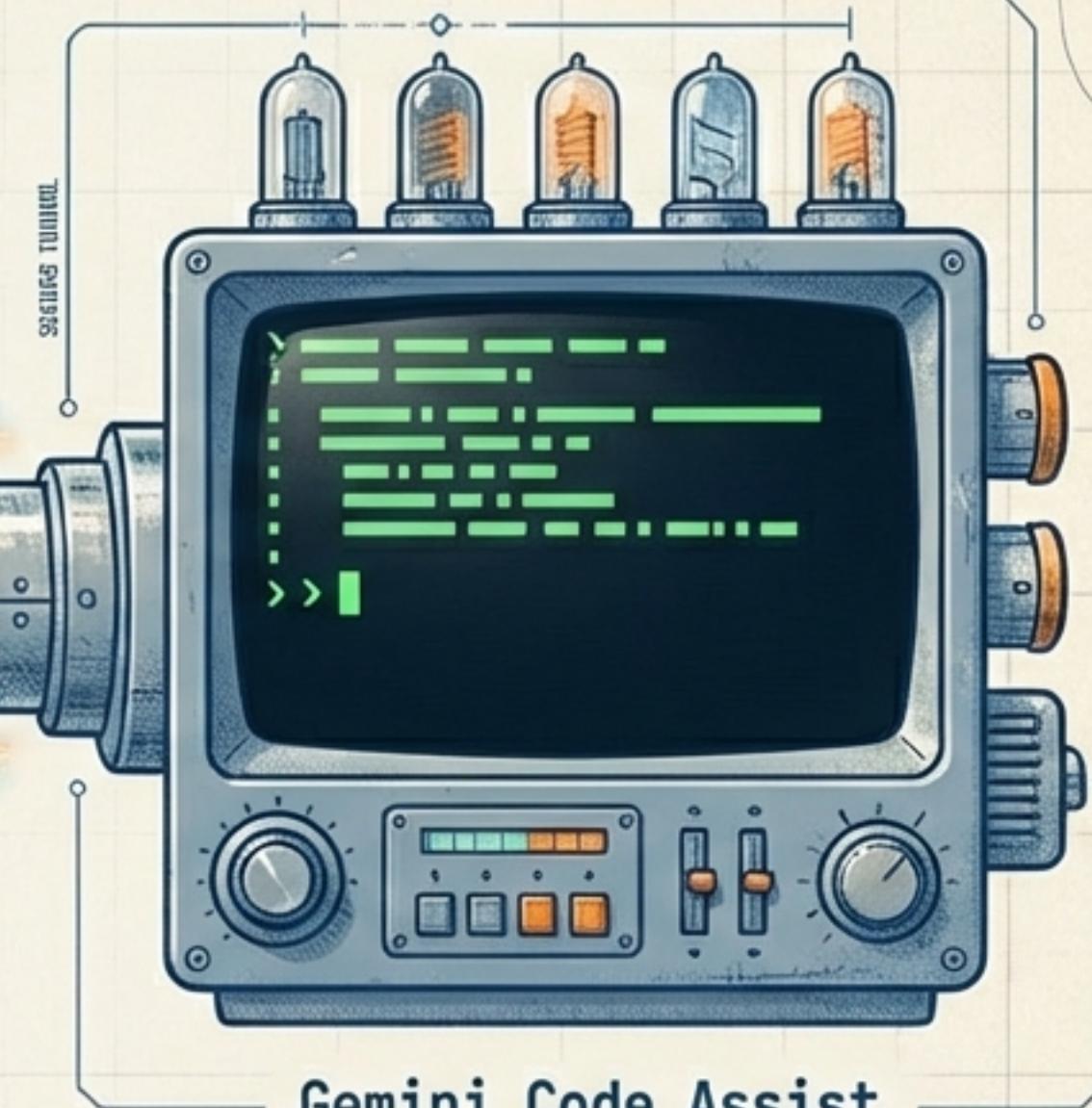
程式碼開發的安全防護：Gemini Code Assist

IP 賠償保障 (IP Indemnification)：為生成的程式碼提供智慧財產權賠償保障。



私有代碼庫
(Private Repositories)

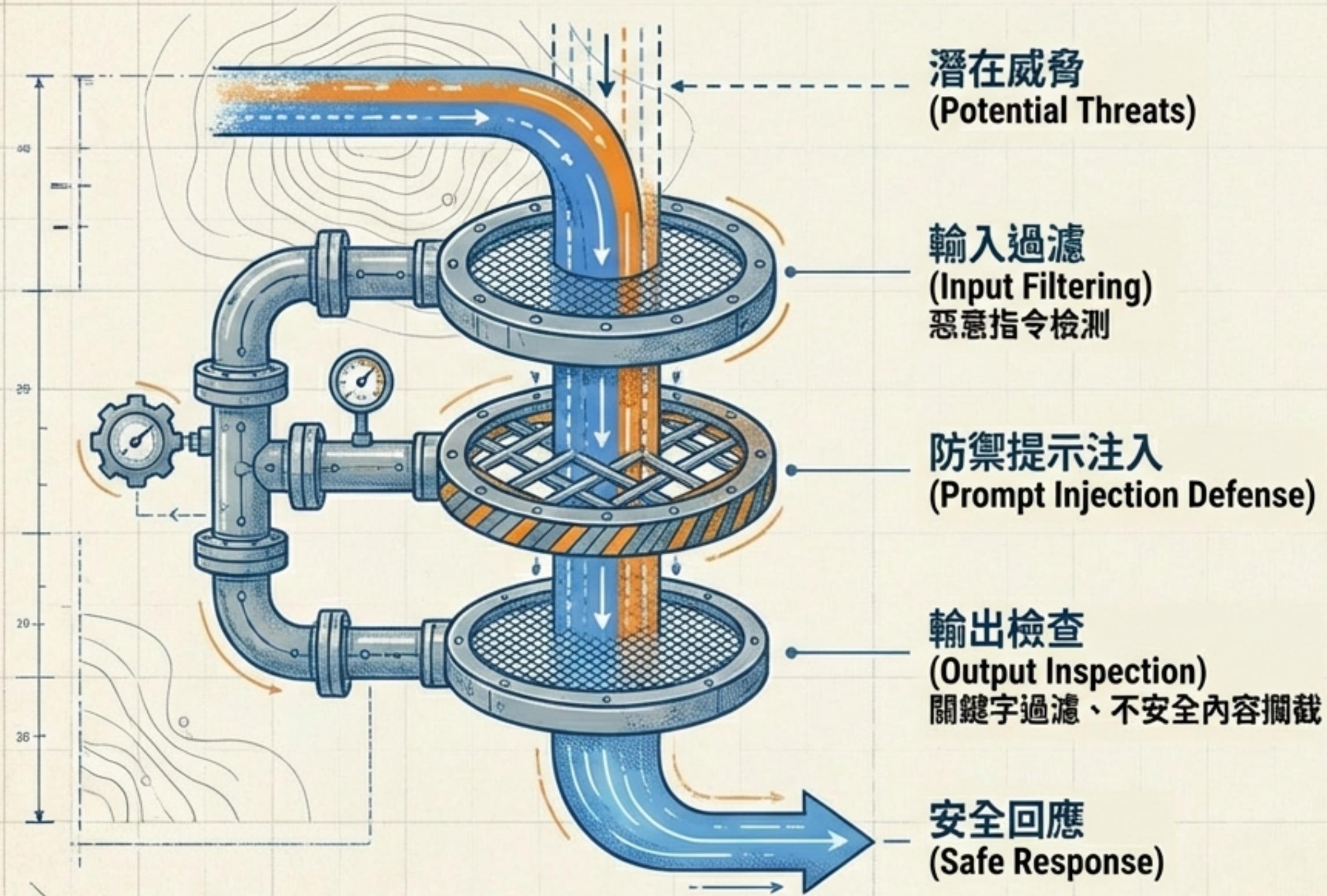
私有代碼庫連接：企業版可連接 GitHub, GitLab, Bitbucket 獲取客製化建議，且不會洩漏代碼給公共模型。



Gemini Code Assist

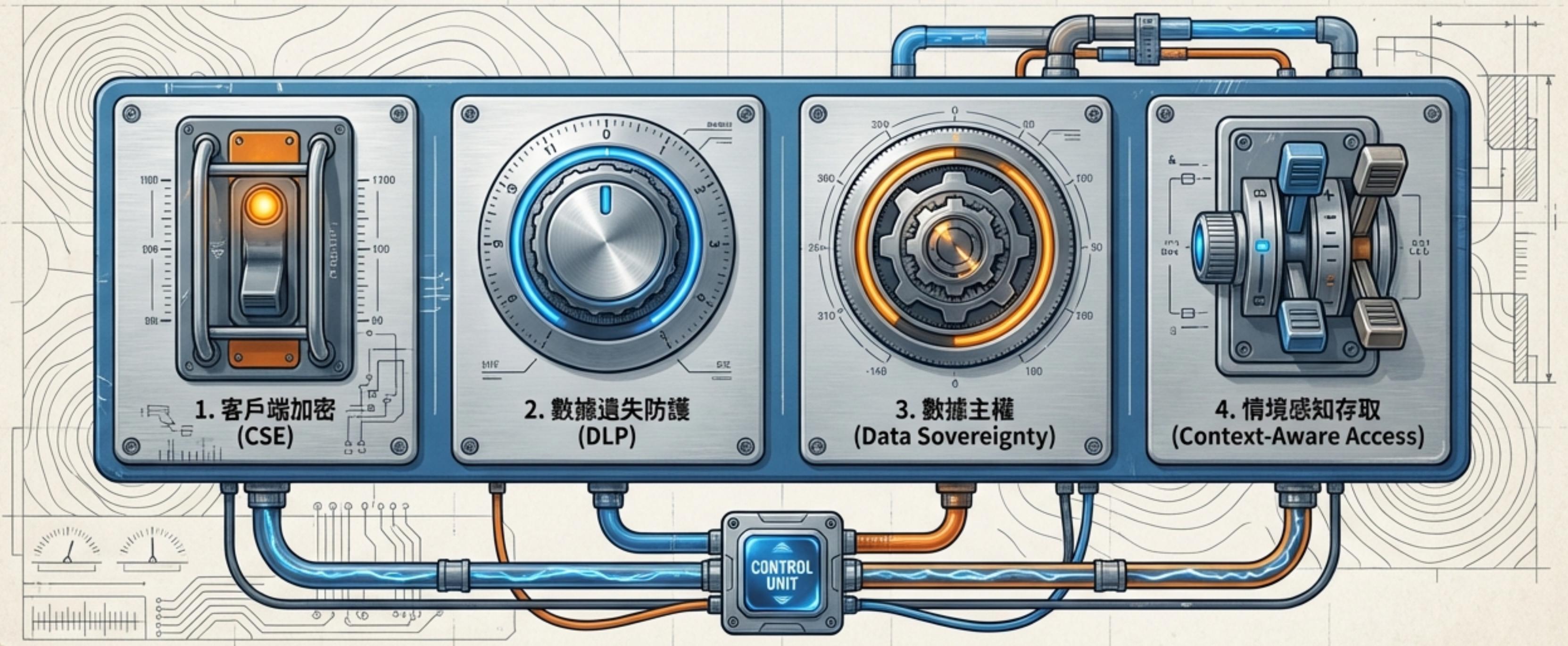
合規性：包含 VPC Service Controls 與 Private Google Access 支援。

防禦新興威脅：分層防禦策略

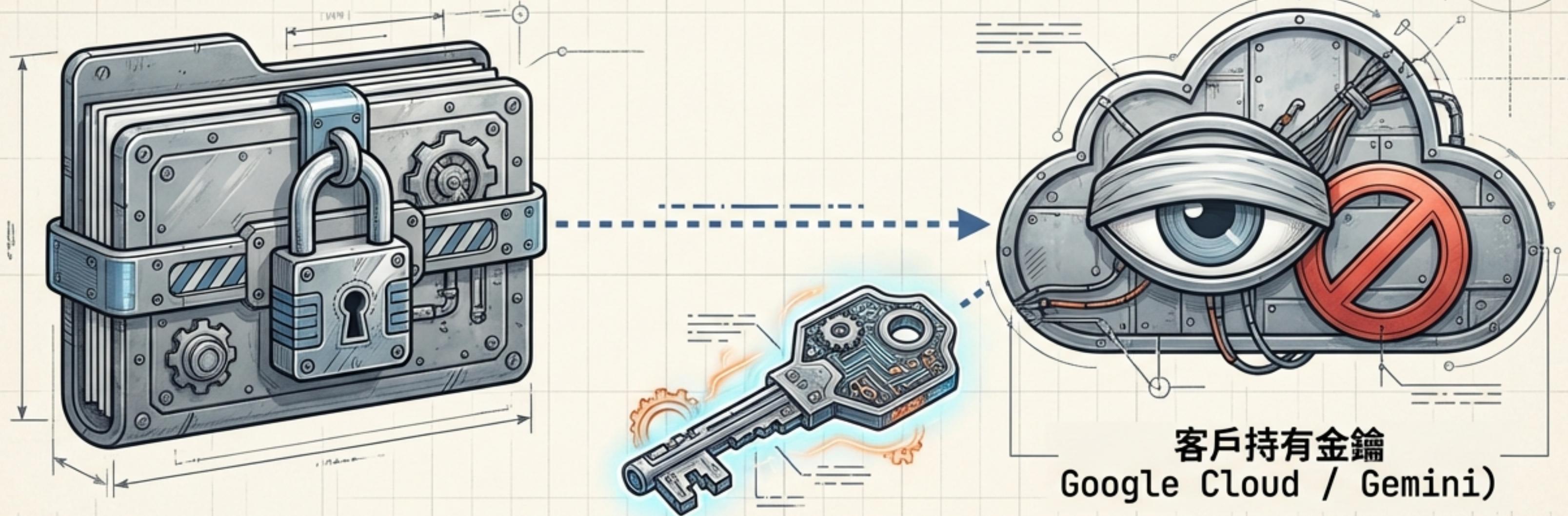


精細化治理：您掌握控制權

雖然 Gemini 預設安全，但我們提供企業級工具讓管理員定義更嚴格的邊界。



終極防護：客戶端加密 (CSE)



加密金鑰由客戶持有，而非 Google。

數據在離開瀏覽器前即被加密，Google 伺服器僅接收到無法辨識的密文。

結果：Gemini 無法檢索或處理受 CSE 保護的文件，確保極機密資訊（如 IP、健康記錄）絕對隱形。

防止數據外洩 (DLP) 與 AI 分類



DLP 規則：自動識別敏感數據（如身分證、信用卡號），禁止輸入至提示詞中，或阻止生成的內容外洩。



AI 自動分類：運用 AI 自動為敏感檔案加上標籤。



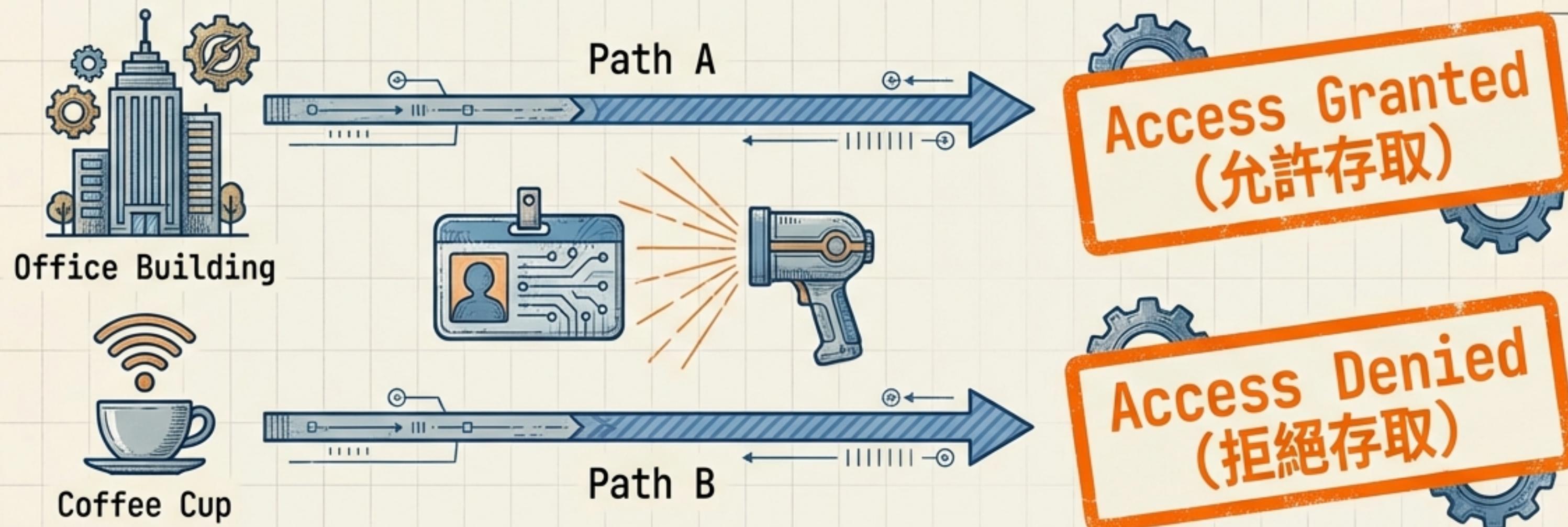
IRM 整合：若文件被標記為禁止複製/列印，Gemini 亦無法讀取該文件內容。

數據主權與區域控制



- 限制處理區域：將 Gemini 的數據處理限制在 美國 (US) 或 歐盟 (EU)。
- 本地資料儲存：可將 Gemini 數據獨立備份於您選擇的國家/地區。
- 支援人員存取限制：限制只有特定地區的 Google 支援人員能存取數據。

情境感知存取 (Context-Aware Access)



- 安全策略是動態且持續的 (Dynamic & Continuous Policies)。
- Gemini 嚴格遵守 Drive/Docs 中的既有權限 (ACLs)。若使用者無權開啟檔案，Gemini 就不會用該檔案回答問題。

業界領先的合規認證

我們的承諾經過第三方嚴格驗證。

SOC 1 / 2 / 3

ISO/IEC 27001
(資訊安全)

ISO/IEC
27701
(隱私資訊)

HIPAA
(醫療合規)

GDPR
(歐盟隱私)

建立 AI 新標準：ISO 42001

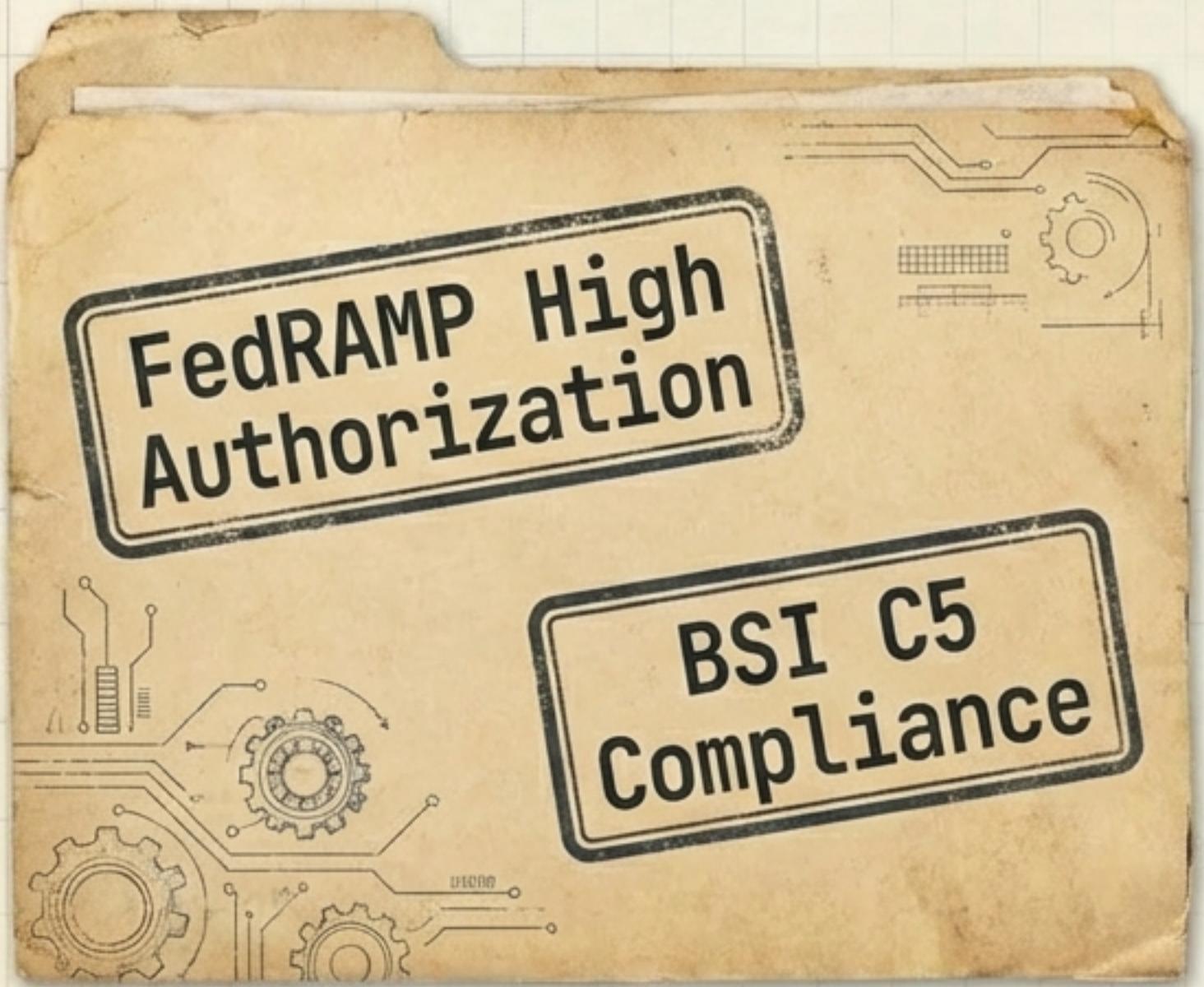


人工智慧管理系統 (AI Management Systems)

Gemini for Workspace 是首個獲得 ISO 42001 認證的生產力與協作套件 AI 助手。
這證明其開發過程是：



政府級安全標準



- ➊ FedRAMP High：獲得美國聯邦政府高安全性數據授權。
- ➋ BSI C5：符合德國雲端運算合規標準。
- ➌ 相比市場其他方案，Gemini 提供更全面的政府級合規認證。

總結：值得信賴的 AI 合作夥伴

[OK] 承諾 (Commitment): 數據歸您所有，不訓練模型
[OK] 架構 (Architecture): 零信任與信任邊界
[OK] 控制 (Controls): CSE 加密與 DLP 防護
[OK] 認證 (Compliance): ISO 42001 與 FedRAMP High

信任 Google Cloud 助您開啟安全無虞的 AI 之旅。

SYSTEM READY.