Onsites AI

SECURITY WHITEPAPER · EDITION 2.0

安全與資料駐留白皮書

資料在誰手裡，寫清楚

加密、訪問控制、審計、備份與刪除時間線、AI 資料邊界與漏洞披露，逐項寫明做法與責任方。不寫「企業級安全」這類無法驗證的形容詞。



版本	釋出	適用範圍	文件編號
第 2.0 版	2026 年 11 月	雲端 · 專屬雲 · 地端	ONS-SC-TW-2.0

© 2026 Onsites AI · 本文件隨產品迭代更新，最新版本見 onsitesai.com/tw/download.html

目錄

CONTENTS

01 **處理角色與資料邊界** 誰控制、誰處理、AI 能碰到什麼 …… 03

02 **加密、訪問控制與審計** 九個控制點的具體做法 …… 04

03 **駐留、備份與生命週期** 資料放在哪、留多久、怎麼刪 …… 05

04 **安全問卷與披露流程** 常見問答、漏洞披露、聯絡方式 …… 06

摘要

Onsites AI 把客戶資料當作客戶託付的資產。雲端與地端兩條路線都具備加密、訪問控制與審計記錄；選擇地端時，全部資料可以留在你自己的網路內。本文件逐項說明九個控制點的做法，並寫明哪些由我們負責、哪些由客戶負責——安全評估最怕的不是「有漏洞」，而是「說不清邊界」。

9 項	TLS 1.3	1 個工作天	3 種形態
內建控制點 可逐條對應問卷	全站傳輸加密 靜態儲存同樣加密	安全報告 確認時限	雲端、專屬雲、 地端各自邊界

九個控制點一覽

01 傳輸
TLS 1.3

02 靜態
儲存介質加密

03 金鑰
與資料分開存放

04 許可權
按席次授權，可收窄為只讀

05 隔離
工作區之間互不可見

06 分享
外鏈可設有效期與次數

07 審計
操作人、時間與細節

08 備份
付費工作區自動備份，可匯出

09 AI 邊界
只讀本工作區，不回訓

文件用途
供安全評估、供應商問卷與合規審查使用，可作為答覆附件直接提交。

適用範圍
雲端 SaaS、商業版 · 專屬雲與地端部署三種形態；差異處已單獨標註。

宣告
本文件描述產品內建能力，不等同於第三方認證。等保、行業合規測評需另行委託。

版本與回饋
第 2.0 版，2026 年 11 月。勘誤與安全報告請傳送至 support@onsitesai.com。

01

ROLES & BOUNDARY

誰控制、誰處理、AI 能碰到什麼

安全評估的第一個問題是角色：資料是誰的，誰在處理，處理過程中會不會交給第三方。Onsites AI 的角色劃分很直接——客戶是控制者，我們是處理者，子處理者只有基礎設施與模型兩類，且隨部署形態變化。

1.1 三種角色

控制者

客戶（你）

決定收集什麼、儲存多久、給誰看。工作區內的席次、角色與許可權由你配置；匯出與刪除也由你發起。

處理者

Onsites AI

按你的配置處理資料：儲存、檢索、生成草稿與單據。不將資料用於自身目的，不跨工作區複用。

子處理者

基礎設施與模型

雲端形態下為雲基礎設施與我們呼叫的模型服務；地端形態下這兩類由客戶自己提供，我們不持有。

1.2 一次 AI 呼叫的四個邊界點

邊界內

工作區資料

會話、客戶、單據、檔案。只有本工作區的成員按許可權可見。

檢索時

許可權過濾

按發起人的席次許可權裁剪可讀範圍；無權訪問的記錄不進入上下文。

推理時

模型呼叫

僅傳輸本次所需的最小上下文；地端可指向內網端點，資料不出網。

返回後

答案與出處

結果標註引用的記錄；不寫入訓練集，不跨工作區複用。

圖 1-1　四個邊界點。任何一環預設，都不應把資料送進模型——這也是我們只讀本工作區、且每條答案都要求標註來源的原因。

1.3 四條 AI 使用邊界

- **只讀本工作區。**Copilot、Harness、Agent Studio 與 Desk 在三種部署形態下都只讀取當前工作區的資料，不跨工作區檢索。
- **回答帶出處。**每個答案標註它引用了哪條會話、哪個客戶欄位或哪份檔案，便於複核；引用不到的，不寫進答案。
- **不用於訓練。**客戶資料不會用於訓練共享或公開模型。地端部署下模型與金鑰完全由客戶提供，預設不出內網。
- **可整體關閉。**AI 能力可按工作區或成員關閉，關閉後其餘功能完全正常，不進入降級狀態。

1.4 三種形態下的角色差別

環節	雲端 / 專屬雲	地端部署
基礎設施	我們運營；專屬云為獨享執行個體	客戶自有機器與網路
模型與金鑰	平台統一呼叫，金鑰由我們管理	客戶提供端點與金鑰，我們不持有
資料位置	Onsites 基礎設施；專屬雲可選區域	客戶機房或私有云，可完全離線

同一套軟體、同一套功能；角色劃分的差別只來自「誰提供基礎設施與模型」。

關於「我們看不看得到」　雲端形態下，運維人員為排障可能接觸到脫敏後的日誌與錯誤資訊；會話正文與附件不作為日常運維物件。若這一點不可接受，地端部署是更徹底的選擇——資料完全不出你的網路。

02

CONTROLS

九個控制點，逐項落到做法

安全問卷通常按控制點逐條問。下面按「加密 → 訪問 → 記錄 → 分享 → AI」的順序給出做法與責任方，可以直接對照填寫；三種形態的差異單獨標註。

2.1 加密與金鑰

環節	做法	誰負責
傳輸	全站 TLS 1.3；地端由你的閘道器終止 TLS，證書由你管理	雲端我們配置；地端客戶配置
靜態儲存	在我們基礎設施上靜態儲存時加密；地端時磁碟加密由你的作業系統與儲存層完成	雲端我們；地端客戶
金鑰管理	金鑰與資料分開存放，僅平台團隊可訪問	雲端我們；地端客戶持有
備份介質	備份檔案同樣加密；備份目標位置由部署形態決定	見第 3 章

2.2 訪問控制

- **按席次授權。**誰能看到什麼由席次與角色決定；角色可收窄為只讀，用於財務與管理層檢視。
- **工作區隔離。**各工作區之間相互隔離，資料不跨工作區流動，AI 檢索同樣受限。
- **收回即時生效。**移除席次即同時收回訪問權，不需要額外操作。
- **檔案分享控制。**私有檔案與資料夾，按受眾分享給客戶、合作伙伴或同事；外鏈可設有效期與開啟次數上限，並可隨時吊銷。

2.3 審計與可追溯

文件與對話的狀態變更都會記錄操作人、時間與細節：誰把報價發給了客戶、誰改了金額、誰確認了合約。日誌隨其他資料一同匯出，因此幾個月之後仍可作為審批依據，而不是隻在系統裡保留一段時間的「活動流」。Desk 執行的動作同樣寫入日誌——讀了什麼、寫了什麼、花了多少點。

記錄項	內容	用途
狀態變更	單據與對話的狀態流轉	複核審批鏈，回答「這一版是誰發的」
許可權變更	席次與角色的授予與收回	離職交接與審計取證
AI 執行	讀取範圍、寫入結果、點數消耗	確認智慧代理沒有越界

2.4 控制點落在鏈路的哪一段



圖 2-1　控制點沿鏈路分佈。評估時按這四段逐段問，比按功能列表問更容易發現缺口。

怎麼驗證　評估階段可以要求我們按上面三條各給一條真實樣本（脫敏後）：一條狀態變更、一條許可權變更、一條 AI 執行記錄。能給出樣本，比在問卷上勾「是」更有說服力。

03

RESIDENCY

資料放在哪、留多久、怎麼刪

駐留問題通常有三個子問題：資料存在哪個區域、備份保留多久、終止合作後怎麼刪。前兩個可以按部署形態選，第三個取決於你有沒有匯出——這也是我們反覆強調「定期匯出」的原因。

3.1 一條資料的生命週期

建立

寫入工作區

會話、客戶、單據與檔案落在工作區內，按許可權可見。

使用

日常讀寫

團隊與 AI 在同一份記錄上讀寫；每次寫操作留痕。

備份

加密副本

付費雲端工作區自動備份；地端按指令碼執行，介質由你保管。

匯出 / 終止

帶走或刪除

標準格式匯出；刪除請求按流程執行，備份副本按保留策略到期。

圖 3-1　生命週期四段。真正需要提前約定的是最後一段：誰發起刪除、備份副本保留多久、如何確認已刪。

3.2 三種形態的駐留與備份

形態	資料位置	備份	刪除
雲端 SaaS	Onsites 基礎設施	付費工作區自動備份	按請求執行，備份按保留策略到期
商業版 · 專屬雲	可選執行個體與備份區域，開通時固定	自動備份，區域隨執行個體	同上，區域不變
地端部署	你的機房或私有云	按隨授權提供的指令碼執行	由你執行；我們提供步驟與確認清單

區域在開通時固定，之後不會變更；如需遷移區域，按新執行個體遷移處理。

3.3 匯出、降級與保留

- **匯出是權利，不是功能開關。**對話、聯絡人與文件都能以標準格式匯出，不鎖定格式、不收取匯出費。
- **降級不刪資料。**停止儲存包或降低方案後，已存資料保留，按需再續；不會因為降級而丟失歷史。
- **免費版沒有服務端副本。**免費工作區不保留服務端備份，定期匯出即是你唯一的副本——這一點最容易被忽略。
- **刪除要能確認。**我們提供刪除執行記錄與備份到期時間，避免出現「說刪了但備份還在」的爭議。

3.4 保留策略怎麼定

資料類別	建議保留	原因
會話與客戶記錄	與業務同週期	售後與復購判斷都依賴歷史對話，過早清理會丟上下文。
報價、合約與發票	按財稅要求	通常長於會話；編號與金額需可複核，版本要留舊檔。
審計日誌	長於單據本身	審批與爭議處理需要「誰在什麼時候改了什麼」。
備份副本	短於主資料	備份只為恢復，不必長期保留；到期即失效，避免刪除爭議。

以上是通用建議；實際保留期以你所在行業的監管要求為準。

建議寫進合約的三個時間　① 資料匯出可用的天數（終止後多久仍可取回）；② 備份副本的保留期；③ 刪除完成後的書面確認時限。把這三個數字寫清楚，比在問卷裡勾「支援資料刪除」有用得多。

04

QUESTIONNAIRE

安全問卷速查與漏洞披露

下面是供應商問卷裡出現頻率最高的幾條，答案可以直接引用；更細的問題歡迎來信，我們會按你的問卷格式逐條填寫，而不是回一份通用宣傳材料。

4.1 常見問題

問題	答覆
資料是否用於訓練模型?	不。AI 只讀本工作區資料，不用於訓練共享或公開模型；地端下模型由客戶提供，資料預設不出內網。
是否支援指定資料儲存區域?	商業版 · 專屬雲可指定執行個體與備份區域，開通時固定；雲端為標準區域；地端由客戶決定。
員工能否看到客戶會話內容?	雲端運維出於排障可能接觸脫敏日誌；會話正文與附件不作為日常運維物件。需要更徹底的隔離請選地端。
是否有審計日誌? 能否匯出?	有。狀態變更、許可權變更與 AI 執行均記錄操作人、時間與細節，可隨資料一同匯出。
檔案外鏈能否限制與吊銷?	可以。按受眾分享，設定有效期與開啟次數上限，隨時吊銷。
終止合作後資料怎麼處理?	以標準格式匯出；刪除按流程執行，我們會提供執行記錄與備份到期時間。
AI 用量能否設上限?	可以。預設軟性上限（接近額度時提醒、不中斷），可改為硬性上限，達到即停止呼叫；點數用完時扣費自動暫停。
地端環境能否離線升級?	可以。新版本以離線包交付，匯入後按引導升級，不要求部署機聯網啟用。

4.2 漏洞披露

STEP 01
報告
傳送至 support@onsitesai.com，直達開發該產品的團隊。

STEP 02
確認
一個個工作天內確認收到，並給出初判與聯絡人。

STEP 03
修復
按影響分級排期修復；期間保持進度同步，不等到釋出才通知。

STEP 04
覆盤
修復釋出後同步結論；如涉及客戶側動作，會給出明確的操作清單。

圖 4-1　披露流程。我們不設漏洞賞金，但會對報告者致謝（除非要求匿名）。

4.3 需要更多材料

如果你的評估需要特定格式的問卷回填、滲透測試報告或地端環境的架構確認書，請直接說明格式與截止時間。地端部署的客戶還可以要求提供部署架構確認書，用於內部安全評審歸檔。

4.4 相關文件

文件	編號	用途
產品手冊	ONS-PM-ZH-2.0	產品構成、能力範圍、部署形態與價格結構（21 頁）。
地端部署指南	ONS-SH-ZH-2.0	地端的適用場景、架構、資源與費用（6 頁）。
安全與資料駐留白皮書	**ONS-SC-TW-2.0**	本文件，供安全問卷與合規審查使用（6 頁）。

三份文件均可從 onsitesai.com/tw/download.html 免費下載，不留表單。

聯絡方式　安全與合規：support@onsitesai.com（安全報告走同一地址，一個個工作天內確認）
產品與文件：onsitesai.com/tw/download.html　·　地端評估：onsitesai.com/tw/self-host.html