

绿区专案 — 需求书 (RFP)

绿区专案 — 需求书 (RFP)

面向供应商的功能与技术要求

甲方: ZD 数位转型委员会

文件类型: *Request For Proposal* (需求书)

v1.0 · 2026-07-27 · ZDT CONFIDENTIAL

4 模块 + 1 跨模块 = 83 项功能要求 (FR)

一、背景說明

背景說明

- 1. ZD 集團擬建設「綠區」—— 一個僅允許受控 AI 服務與企業管控桌面進入的安全工作區
- 2. 現狀：員工透過個人 AI 帳號（ChatGPT / Claude 等）處理公司資料，數據外洩風險高
- 3. 挑戰：缺乏統一 AI 入口、敏感資料無法審計、AI 輸出無 DLP 防護

目的

- 1. 建立綠區統一入口，杜絕個人帳號 / 未授權 AI 服務進入
- 2. 提供完整的 DLP、ACL、審計日誌，滿足合規要求
- 3. 支援開發者 Vibe Coding / Agent 編排，同時不犧牲安全

效益分析

- 1. 降低數據外洩風險，提升甲方合規等級
- 2. 提升開發者 AI 生產力（多模型路由 + 統一接口）
- 3. 建立可審計、可追溯的 AI 使用記錄體系
- 4. 為後續 AI 治理（如 RBAC 模型控制）奠定基礎

ZDT Confidential

二、需求範圍（4 模組 + 1 跨模块）

綠區 4 大核心模組：

VDI

虛擬桌面基礎設施

13 項 FR

剪貼簿隔離 · 螢幕浮水印 · 檔案審核 · 桌面持久化 · 視訊音訊雙向

LLM Gateway

AI 統一網關

22 項 FR

模型路由 · 跨平台調用 · Prompt 注入防禦 · DLP · ACL · 日誌

CSP

Cloud Service Platform

18 項 FR

AI 網站 SSO · 個人帳號屏蔽 · 聊天隔離 · 統一 base_url · 配額限流

AI Browser

企業管控瀏覽器

20 項 FR

網址白名單 · 書籤預設 · DLP · 自動登入 · 防繞過

跨模块串接

10 項 FR — VDI → AI Browser → CSP → LLM Gateway → 外部 CSP/Meeting Server 全鏈路驗證

合計 83 項功能要求（FR）覆蓋完整綠區方案

三、綠區系統架構圖

已審核 CSP / 模型廠

OpenAI · DeepSeek · Anthropic · AvaryGPT

已審核 Meeting Server

甲方 ATP / ATPS [TBD] · 其他 ✕ 阻斷

綠區邊界

LLM Gateway

統一入口/中轉站
開發者模型路由
Meeting 導線

Web Proxy

URL 白名單
CSP 域名過濾
流量方向控制

企業瀏覽器

DLP 防洩
上傳/下載攔截
複製貼上控制

檔案審核通道

VDI 配套
頂家/TBD 或 OA 審核
主管雙向通知

VDI Server (綠區內核)

按身份派發桌面 (員工 / 開發者 / 外部訪客) · 音視訊雙向支援 · 檔案上傳走審核

① 一般使用者

員工桌面 · AI Chat · 走雙開

② 開發者

Vibe Coding · Agent 編排 · 走 Gateway

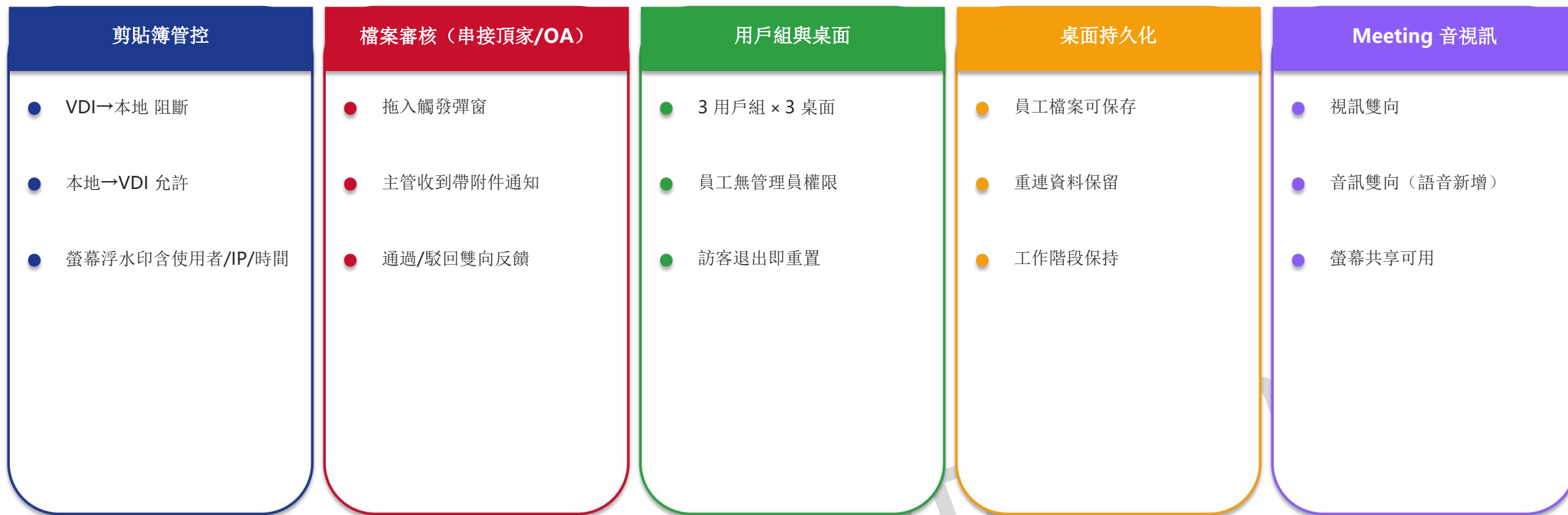
③ 特殊使用者

外部訪客桌面 · Meeting 視訊

圖例: 綠色=已審核 CSP / 橘色=Meeting Server / 藍色=LLM Gateway / 青色=雙開 / 粉=檔案審核

四、VDI 需求 (13 項 FR)

VDI = 虛擬桌面基礎設施，承載員工 / 開發者 / 外部訪客的桌面環境



VDI 模組共 13 項 FR (必要項)，含 1 項語音新增 (音訊傳輸)

關鍵驗證：水印含三要素 · 剪貼簿單向 · 檔案審核帶附件通知 · 桌面權限嚴格

五、LLM Gateway 需求（22 項 FR）

LLM Gateway = AI 統一入口，提供模型路由 / DLP / ACL / 日誌

模型路由

- 雲/地端自由切換
- model 參數路由
- 自動路由備援

跨平台調用

- 瀏覽器 Chat UI
- Vibe Coding (VS Code)
- Agent / MCP 調用

Prompt 注入防禦

- 直接越獄攔截
- Base64 編碼識別
- 多輪漸進標記
- Agent 間接注入

DLP（雙側）

- 輸入側 PII 遮罩
- 輸出側敏感詞過濾
- 企業機密檢測
- 完整對照日誌

ACL + 配額

- 4 類 Token（開發者/用戶/SA/管理員）
- QPS 速率限制
- 用戶/部門配額
- RBAC 控模型/Agent/MCP

日誌 + 審計

- 調用全字段記錄
- 注入獨立安全日誌
- DLP 專項日誌
- 可匯出可追溯

LLM Gateway 共 22 項 FR（功能 4 / 管理 7 / 防護 4 / 日誌 4 / ACL 3）

關鍵驗證：中美模型並存路由 · 雙側 DLP 不遺漏 · 注入 4 種手法全部攔截

六、CSP 需求 (18 項 FR)

CSP = AI 網站 SSO 代理 + base_url 統一入口

AI 網站 SSO

- 免登錄自動登入
- 個人帳號入口屏蔽
- 無痕模式仍企業登入
- 次日會話保持

聊天記錄隔離

- 員工間不可見
- 管理員僅見用量
- 跨設備同步
- 本地獨立儲存

統一 base_url

- Vibe Coding 接入
- Agent 編排接入
- OpenAI 協議相容
- 模型清單可擴展

配額 + 限流

- 按用戶/部門配額
- 超額即時攔截
- RPM/TPM 限流
- 配額預警通知

CSP 共 18 項 FR (SSO 3 / 隔離 4 / 統一 4 / 配額限流 7)

關鍵驗證: 員工互不可見 / 管理員不見內容 / 個人帳號 100% 屏蔽

七、AI Browser 需求 (20 項 FR)

AI Browser = 員工進入 AI 網站的唯一瀏覽器 (雙開之一)

網址白名單

- 白名單放行
- 非白名單攔截+提示
- 管理員即時增刪
- 無需重啟生效

書籤預設

- 雲端 AI 書籤
- 地端 AvaryGPT 書籤
- 點擊即達
- 員工不可修改

DLP 防洩

- 貼上敏感詞攔截
- 上傳敏感檔攔截
- PII 脫敏提示
- 輸出側警告

聊天隔離

- 員工間不可見
- 管理員僅見用量
- 跨設備同步

CSP 自動登入

- 點書籤免登入
- 立即可對話
- 次日保持登入

防繞過

- 禁用其他瀏覽器
- 開發者工具鎖
- 白名單不可繞過

AI Browser 共 20 項 FR (白名單 4 / 書籤 3 / 隔離 3 / DLP 4 / SSO 3 / 防繞 3)

關鍵驗證: 員工 100% 只能透過此瀏覽器進入 AI 網站 · 開發者工具鎖定

八、跨模块串接 + 驗收方式 (10 項 FR)

4 條主鏈路 + 4 階段驗收 — 任一單點達標但鏈路不通都視為不通過

4 條主鏈路

SSO 鏈路

AI Browser → CSP → AI 網站

多模型

AI Browser → CSP → 各 AI 網站

VDI 完整鏈

VDI → AI Browser → CSP → AI

開發者鏈

VDI → VS Code → CSP base_url → Gateway

4 階段驗收

階段一

所有「應」項 100% 通過

單模組功能驗收

階段二

FR-XMOD-01~10 全部通過

跨模块鏈路驗收

階段三

第 7.2 節合規全部達標

安全合規驗收

階段四

≥ 30 天無 P0/P1 故障

試運行

跨模块共 10 項 FR，分階段驗收 • 乙方需駐場至階段二通過

九、交付物總覽 + 下一步

通用交付物（乙方應隨產品提供）

架構文檔	含 4 模組 + 跨模块拓撲圖
API 接口文檔	OpenAPI / Swagger 或等價物
部署運維手冊	完整安裝/升級/備份流程
安全合規白皮書	DLP 規則 / 注入策略依據
用戶操作手冊	VDI / Browser / CSP / Gateway 各一份
故障排查手冊	常見問題 + 排查流程圖
產品滲透測試報告	最近 12 個月內

下一步行動（ZD 委員會）

● v0.1 → v0.2	確認 TBD 7 項: ATP/ATPS · 頂家 · 上傳方向 · 視訊關係 · 外部專線 · 雙開次序 · Vibe 走法
● T+7 天	PoC 測試項清單最終版（已合併至 33 項端點+傳輸 + 6 sheet）
● T+14 天	招標啟動 · 邀請乙方投標 · 提供 RFP v1.0
● T+30 天	PoC 實測 · 5 廠商橫評（TrustOne / 飛馳雲聯 / IPG / PA / 亞信）
● T+45 天	PoC 結果彙整 · 委員會決議 · 簽約