
政企本地化 AI 办公平台

行业白皮书

版本 v1.0

2026 年 6 月

目录

摘要	1
一、行业背景：AI 办公浪潮与政企的数据主权诉求	1
二、政企智能办公的四大挑战	1
三、解决思路：本地化的一体化 AI 办公工作台	2
四、产品总览：「数智 AI 一体机」平台	2
4.1 智记——会议录音分析	2
4.2 智写——公文撰写	3
4.3 智问——AI 对话	3
4.4 智库——知识库	3
4.5 智档——平台文件管理	3
4.6 控制台——用户与权限	3
五、关键技术特性	3
六、安全与合规	4
七、典型应用场景	5
八、价值与收益	5
九、部署与实施	5
十、展望	6
结语	6

摘要

生成式 AI 正在重塑办公方式，但对党政机关、国资央企、金融、法律、医疗等数据敏感单位而言，「把公文、会议录音、内部资料喂给公有云大模型」是一条无法逾越的合规红线。这些单位面临一个共同的两难：**既要 AI 带来的效率，又不能让数据出域。**

本白皮书分析政企智能办公的行业趋势与核心挑战，提出「**本地化部署 + 一体化工作台 + 细粒度权限**」的解决思路，并以「数智 AI 一体机」平台为样本，说明如何在**数据全程不出内网**的前提下，把开会记录、公文撰写、信息问答、知识沉淀、文件协作五类高频工作交给 AI 协助完成。核心结论：政企 AI 落地的关键不在于模型多大，而在于**能否在单位自有算力上、以可控的权限和可审计的方式，安全地用起来。**

一、行业背景：AI 办公浪潮与政企的数据主权诉求

近两年，大语言模型（LLM）、语音识别（ASR）、向量检索等技术成熟，“AI 办公助手”快速普及。文档起草、会议纪要、智能问答等场景，效率提升以倍计。

但主流 AI 办公产品大多是**公有云 SaaS 形态**——数据上传到厂商云端处理。这对消费者和一般企业无妨，对政企单位却存在结构性冲突：

- **数据主权：**公文、内部制度、会议内容属于单位核心资产乃至涉密信息，按规不得出域、不得交第三方留存。
- **合规要求：**《数据安全法》《个人信息保护法》及行业主管部门的等保、信创要求，对数据存储位置、处理方式、可审计性都有硬性约束。
- **信创趋势：**关键信息基础设施的国产化、自主可控，要求软硬件可在内网独立运行，不依赖外部云服务。

结果是：**越是需要 AI 的高价值单位，越不敢用云上的 AI。**行业亟需一种”能力不打折、数据不出门”的落地形态。

二、政企智能办公的四大挑战

挑战	表现	后果
数据不能出域	公文、录音、资料无法上传公有云	主流 AI 工具直接出局
工具碎片化	转写、写作、问答、网盘各用一套，账号与数据彼此割裂	资料反复搬运，沉淀不下来，AI 也”看不到全局”

挑战	表现	后果
权限粗放	共享资料”一放就全员可见”，或”一锁就谁也用了”	协作与保密二选一，落地受阻
沉淀与复用难	历次会议、历史文档散落各处，查找靠人脑和翻文件	组织知识无法转化为可检索、可问答的资产

这四点叠加，使得政企”用 AI”常停留在试点，难以规模化。破局需要一个**统一、本地、可管控**的平台底座。

三、解决思路：本地化的一体化 AI 办公工作台

针对上述挑战，本白皮书主张三条设计原则：

- 1. **本地化优先 (Local-First)**：语音转写、大模型、向量检索全部私有部署，运行在单位自有服务器，**资料不上传任何第三方云**，原件落在单位自有磁盘、纳入既有备份。
- 2. **一体化工作台 (All-in-One)**：会议、公文、问答、知识库、文件管理收敛到**同一个登录入口与同一套数据底座**，一次登录全程通行，资料一处沉淀、处处可用。
- 3. **细粒度可管控 (Governed)**：内置多用户、角色、用户群组、按文件夹授权与数据隔离，配合全员操作日志审计，让”协作”与”保密”不再二选一。

「数智 AI 一体机」平台即这一思路的工程化落地。

四、产品总览：「数智 AI 一体机」平台

打开浏览器即用、无需安装客户端。登录后进入一个**类操作系统的桌面**（“数智 AI 一体机”）：底部 Dock 切换应用、顶栏看时间与动态提醒、右侧实时显示系统运行状态。平台由六大模块构成：

4.1 智记——会议录音分析

把一段会议录音变成可检索、可复用的结构化资料。- 上传即转写：常见音频格式自动转成**带时间戳、分说话人的文字稿**。- 波形回放：转写稿按句分段并配波形条，**点某句即定位录音播放、当前句高亮**，边看文字边听原声。- 说话人整理：「说话人 1/2/…」可改成真实姓名（从通讯录选人或手输），识别误拆成多人时还能**筛选核对并合并纠正**，随时可还原，不破坏原始识别。- 一键纪要：AI 自动生成会议纪要。- 沉淀可问：转写内容自动建立语义索引，之后可在”智问”里直接对这场会议提问。

4.2 智写——公文撰写

面向公文、报告、通知等正式文稿的 AI 写作助手。- 多写作场景：可指定文种、语言风格、字数要求。- 生成与改写：按要点生成初稿，或对已有内容润色、续写、改写、扩写。- **文档校对**：一键查错——错别字、标点、语法、用词、数字、公文格式、敏感表述按需勾选；逐条列出「原文 → 建议 + 原因」，点条目即定位到正文，可单条采纳或一键全部采纳。- 富文本精修 + 历史留存：每篇自动归档，随时回看再编辑。

4.3 智问——AI 对话

一个会”读你资料”的对话助手。- 流式回答，逐字呈现。- **按需挂载知识（RAG）**：对话里勾选”范围”，把指定知识库或会议作为参考来源，AI 基于你的资料作答。- 对话里发文件：文档（PDF/Word/TXT/Markdown）随问随查，图片交给多模态模型直接”看”，附件挂在消息上、整场可继续追问。- **来源可溯**：回答标注引用了哪些资料片段，结果可核查。- 多会话管理：按主题分开、按日期分组、标题可重命名。

4.4 智库——知识库

团队资料的统一归集与智能检索底座。- 多格式入库（PDF/Word/TXT/Markdown），不支持类型即时提示、失败文档一键重试。- 自动切分、建立语义索引，入库即可被”智问”检索。- 分库管理：我创建的 / 我订阅的 / 发现公开；公开库可被他人订阅（只读）。

4.5 智档——平台文件管理

团队共享文件库，像网盘一样组织资料，并按**文件夹精细授权**。- 多级目录树、面包屑、上传/新建/重命名/移动（含拖拽）、同名自动加后缀。- 大文件分片上传 + 进度 + 断点续传；整文件夹（含子目录）一次拖入保留结构。- **按文件夹授权**：禁止访问 / 只读 / 可读写，子目录默认继承；深层授权可从”授权目录”入口直达。- 标签筛选、收藏、在线预览、回收站（软删除可恢复，确认后彻底清除）。- **内容提取（文档电子化）**：Word/PDF/图片一键转可复制纯文本，原生文档无损解析、扫描件走 OCR（保表格版式），结果可查看 / 复制 / 下载为.txt。

4.6 控制台——用户与权限

管理员专属入口（普通成员不可见）：用户账号、用户群组、文件夹权限编辑、**日志中心**（检索全员操作日志）。

五、关键技术特性

能力	说明	对政企的意义
全私有部署	语音转写、大模型、向量检索均为可自部署服务，按算力灵活配置	数据不出内网，自主可控

能力	说明	对政企的意义
检索增强生成 (RAG)	文档/会议自动向量化，问答按勾选范围检索本单位资料并标注出处	AI 答案有依据、可溯源，不”一本正经胡说”
向量语义检索	文档与转写切块向量化，按语义相似度近似最近邻检索	跨文档、跨会议”按意思找”，而非关键词死磕
多模态对话	文档随问随查、图片直接”看”（需多模态模型）	一个入口处理文本与图像材料
细粒度权限模型	按文件夹的用户级/群组级 ACL（禁止/只读/可读写），子目录继承、就近取严	协作与保密兼得
数据隔离	会议、文稿、对话、私有知识库按归属隔离，越权不可见	成员资料互不串门
大文件可靠传输	自动分片、断点续传、整文件夹保结构上传	大体量资料归集无忧
全员操作审计	操作日志按分类/操作人/内容/时间检索分页	留痕可查，满足合规

技术选型与实现细节（FastAPI 后端、PostgreSQL + pgvector 向量库、JWT 鉴权、本地 LLM/ASR/Embedding 服务、容器化交付等）见 ARCHITECTURE.md。

六、安全与合规

数据安全是政企采用 AI 的前置条件，而非附加项。本平台从三个层面构建安全基线：

- **部署层·数据不出域**：所有 AI 能力本地/私有部署，资料不上传第三方云；平台可整体部署在单位内网，数据不出网络边界。
- **存储层·原件本地留存**：上传的音频、文档、文件原件落在单位自有服务器磁盘，按相对路径与唯一命名管理，规避重名覆盖与路径穿越，可纳入既有备份与灾备策略。
- **访问层·鉴权 + 权限 + 审计**：
 - 全部业务接口统一登录门禁，无有效凭据一律拒绝；登录态有效期可配置。
 - 管理员/普通成员双角色；按文件夹的用户级与群组级授权；成员业务数据相互隔离。
 - 日志中心留存全员操作记录，可按分类、操作人、内容、时间范围检索，满足留痕与可审计要求。

这套基线对齐数据安全相关法规与等保、信创的总体方向，为单位在内网安全用 AI 提供可解释、可核查的支撑。

七、典型应用场景

党政机关 / 事业单位 - 会议录音转写 + 一键纪要，点句回放核对原声；公文起草、润色与合规校对（错别字、敏感表述、公文格式）一站完成。

法律 / 合规部门 - 制度、案卷、合同入库为知识库，问答时挂载相关库与会议、答案标注出处；按“项目—组别”分文件夹授权，深层目录直达、无关人员不可见。

金融 / 国资央企 - 内部材料不出内网即可被 AI 检索问答；多用户群组按部门授权，操作全程留痕审计。

制造 / 科研 / 医疗 - 技术文档、规程、研究资料沉淀为可检索知识；大体量文件分片可靠归集；图文材料经多模态对话辅助理解（需多模态模型）。

共性价值：把“散落的资料 + 私有的算力”组合成一个会回答问题、能安全协作的组织大脑。

八、价值与收益

- **效率**：会议纪要、公文起草、资料查找等高频耗时工作由 AI 协助，单项工序从“小时级”压缩到“分钟级”。
- **质量**：公文校对降低错别字/格式/敏感表述风险；问答有出处、可核查，减少口径偏差。
- **沉淀**：历次会议与历史文档转化为可检索、可问答的组织资产，避免知识随人流失。
- **安全**：数据不出内网、权限可控、操作可审计，让“用 AI”与“守底线”并行不悖。
- **成本**：浏览器访问无需装客户端，前后端容器化交付，复用单位既有算力与内网，降低引入与运维门槛。

九、部署与实施

- **交付形态**：前端、后端均以容器交付，配合内网的数据库与可私有部署的模型服务（语音转写 / 大模型 / 向量模型）一键起停。
- **访问方式**：成员通过浏览器访问统一入口，无需安装客户端；一次登录、各应用免重复登录。
- **算力适配**：模型服务按单位算力灵活配置，可随业务规模横向伸缩。
- **建议路径**：① 内网就绪数据库与模型服务 → ② 部署平台、创建管理员与成员 → ③ 选取 1~2 个高频场景（如“会议纪要”或“公文校对”）试点 → ④ 沉淀知识库、配置文件夹权限 → ⑤ 逐步推广到全员。

十、展望

本地化 AI 办公正从”单点工具”走向”统一底座”。后续演进方向包括：更强的多模态理解、更丰富的公文模板与校对规则库、知识图谱化的资料组织、以及与单位既有 OA/业务系统的对接。其内核不变——**让组织在自主可控的前提下，把数据用成生产力。**

结语

对政企单位而言，AI 的价值从来不只是”更聪明的模型”，而是**能不能在守住数据底线的同时真正用起来**。「数智 AI 一体机」给出的答案是：把六类高频办公能力收敛到一个本地化、一体化、可管控的工作台，让数据不出内网、协作不失边界、知识不再流失。这是一条把”AI 浪潮”稳妥落到政企地面的可行路径。

本白皮书所述功能均对应平台现有能力；行业趋势部分为通用背景分析。技术细节以 ARCHITECTURE.md 为准。