

What is an Enterprise AI License? Does My Organization Need One?

A companion guide to Understanding and Using AI Responsibly, for organizations weighing whether to move from free or individual AI accounts to an enterprise-tier license.

Once staff start relying on AI regularly, organizations face a real decision: stay on free or individual paid accounts, or invest in an enterprise-tier license. For a large corporation this is a simple budget line. For a small civil society organization with a handful of staff and a tight budget, it is a genuine trade-off worth thinking through deliberately.

The Case for an Enterprise License

An enterprise or business-tier plan (as opposed to a free account or an individual \$20/month subscription) typically adds:

- **Data protection by default:** inputs are excluded from model training and are not used to improve the underlying AI, which matters if staff are pasting in draft grant language, HR content, or program data
- **Centralized admin controls:** single sign-on, the ability to see (in aggregate) how the tool is being used, and the ability to immediately revoke access when someone leaves the organization
- **Consistency and oversight:** one sanctioned tool is far easier to govern than a dozen staff quietly using a dozen different free tools with unclear settings, sometimes called "AI sprawl"
- **Higher usage limits and stronger models:** fewer interruptions from rate limits, and often access to more capable versions of the AI
- **Compliance support:** audit logs, data retention controls, and documentation that can matter for funder requirements or legal review

Why Many Small Organizations Hesitate

- **Cost adds up fast:** enterprise pricing is generally quoted per seat, often in a similar range to the ~\$20/month individual tier but with minimum seat counts or contract terms — a real cost for an organization with five or ten staff and a lean budget
- **Procurement overhead:** contracts, data processing agreements, and admin setup take staff time that a small team may not have
- **Uneven staff usage:** if only two or three people use AI daily, paying for enterprise seats for everyone may not be worth it yet
- **Free and individual tiers have improved:** many platforms now let individual paid users opt out of having their chats used for training, closing some of the privacy gap with enterprise tiers, though admin oversight and audit tools still require the enterprise tier

The Privacy and Security Angle

For organizations serving vulnerable populations — immigrants, survivors, litigants, patients, or other communities where a data exposure could cause real harm — privacy and security should weigh more heavily than cost alone.

- On any tier, free or enterprise, staff should never enter names, addresses, case details, or other identifying or confidential information into an AI tool. Treat every AI input as if it could become public.
- Enterprise and business tiers generally guarantee, contractually, that inputs are not used for model training — free tiers may not offer this by default and require staff to manually adjust settings, which is easy to forget
- Centralized admin control means leadership can see which tool the organization is using and turn off access in one place, rather than discovering after the fact that AI sprawl left data scattered across accounts no one is tracking
- If your organization has real subpoena risk or works with especially sensitive information, a privacy-first tool built around end-to-end encryption is worth exploring alongside — or instead of — a mainstream enterprise plan (see Confer, below)

“ **Groundwire's Advice:** Small organizations do not need to choose the most expensive option. A reasonable starting point is: pick one AI tool as your organization's standard, put it on individual paid accounts (with data-sharing settings turned off) while usage is light, and move to an enterprise or business tier once several staff are using AI daily or once you're regularly handling anything sensitive. Whatever tier you choose, pair it with a written AI policy so staff know what they can and cannot enter into the tool.

Comparing Enterprise AI Vendors

Each platform below is compared across the same seven attributes: primary strength, data privacy, admin controls, security, workspace integration, collaboration features, and compliance & governance.

ChatGPT Enterprise (OpenAI)

- **Primary Strength:** Creativity, R&D, coding, content ideation
- **Data Privacy:** Never trains on customer data; data is not used to improve models
- **Admin Controls:** SSO, SCIM, role-based access, usage analytics
- **Security:** Encrypted in transit and at rest; data residency available; no OpenAI staff access to customer data
- **Workspace Integration:** SharePoint, OneDrive, Google Drive, Box, GitHub; custom app integrations via GPTs
- **Collaboration Features:** Shared GPTs, team knowledge base, chat with files (PDFs, spreadsheets)
- **Compliance & Governance:** SOC 2, ISO 27001, GDPR; data residency options

Claude for Business (Anthropic)

- **Primary Strength:** Safe, reliable AI for complex reasoning & code
- **Data Privacy:** Customer data is not used for training; explicit privacy-first design
- **Admin Controls:** Self-serve seat management, spend caps, usage & code analytics, compliance API
- **Security:** Encrypted in transit and at rest; no training on inputs; audit logs and compliance API
- **Workspace Integration:** Google Workspace, GitHub, Slack via API or webhooks
- **Collaboration Features:** Projects & Artifacts (shared workspaces), team prompts & templates
- **Compliance & Governance:** SOC 2, HIPAA, GDPR; compliance API for audit and retention

Gemini for Business (Google)

- **Primary Strength:** Real-time web search & Google Workspace integration
- **Data Privacy:** Workspace data used contextually but not for model training; customers can disable AI data usage
- **Admin Controls:** Admin console, contextual grounding in Drive/Gmail, data regions, DLP controls
- **Security:** Encrypted in transit and at rest; DLP, context-aware access, data region controls
- **Workspace Integration:** Native in Gmail, Docs, Drive, Meet, Calendar ("Gemini in Workspace")

- **Collaboration Features:** Real-time co-editing with AI suggestions, AI-generated meeting summaries in Meet
- **Compliance & Governance:** FedRAMP, HIPAA, GDPR; data regions, eDiscovery

Microsoft 365 Copilot

- **Primary Strength:** Deep integration with Microsoft 365 apps (Word, Teams, Outlook, etc.)
 - **Data Privacy:** Customer data not used to train models; processed within the Microsoft cloud
 - **Admin Controls:** Full M365 admin center integration, conditional access, sensitivity labels
 - **Security:** Encrypted in transit and at rest; Microsoft Zero Trust model; integrates with Defender and Purview
 - **Workspace Integration:** Fully embedded in Word, Excel, PowerPoint, Outlook, Teams, Loop
 - **Collaboration Features:** Meeting recaps in Teams, smart scheduling in Outlook, collaborative drafting
 - **Compliance & Governance:** Full M365 compliance suite; Purview, eDiscovery, sensitivity labels
-

A Privacy-First Alternative to Watch: Confer

A newer category of AI platform is emerging that is built around privacy as the foundation rather than an add-on feature. Confer, launched by Moxie Marlinspike (the creator of Signal), is the leading example. It's worth understanding, though it is not yet a like-for-like substitute for the enterprise platforms above.

- **Primary Strength:** Private, end-to-end encrypted AI assistant — the goal is that no one, not even Confer itself, can see what you say to it
- **Data Privacy:** If Confer were subpoenaed, the government could not see what was shared with it — only that an account exists
- **Admin Controls:** None currently — no team plan or admin console
- **Security:** End-to-end encryption is the core design principle, not an add-on
- **Workspace Integration:** None currently — no file or document upload support
- **Collaboration Features:** None currently — built for individual, non-collaborative use
- **Compliance & Governance:** No compliance documentation available yet
- **Cost:** Roughly \$35/month, individual subscription (not a per-seat enterprise contract)

Groundwire's Advice: Confer is a great option for an individual staff member — an executive director, an attorney, or anyone regularly discussing sensitive matters — who wants a more private alternative to mainstream chatbots for one-off, non-collaborative use. It is not yet ready to serve as your organization's primary, organization-wide AI platform. We recommend watching how it develops and pairing it with, rather than substituting it for, your main enterprise tool.

A Final Word

Whatever combination of tools and license tiers you choose, the constant should be **human review**, a clear written policy, and staff who understand both what AI is good at and where it falls short.

It is also important to keep in mind, that even with an enterprise license, that AI company still stores your data, similarly to the way Google or Microsoft stores your data.

There is no single right answer for every organization — the right tier depends on your budget, how much staff already rely on AI, and how sensitive the information you handle tends to be.

Revision #3

Created 10 August 2026 17:55:59 by Galia

Updated 10 August 2026 18:00:37 by Galia