

Read with the **Security & Data-Handling Brief**. This addendum covers the company-hosted deployment option. Several items below are **available on request** rather than self-serve today; they are marked as such.

1. Deployment on your AWS & your keys

PurposeMapped can deploy the same stack into **your company's AWS account**, using **your enterprise model-provider keys** — one dedicated assistant instance per participating employee. Your organization owns the AWS account, the database, the backups, and the keys. Token spend is billed to your provider accounts. **Available on request** (Company Deployment Kit, IaC-based).

Honesty rule: because your company owns the AWS account, your IT *can* technically reach the instances. We therefore promise **policy + technical separation plus company-defined oversight** — per-employee instance, encryption at rest, no central content store, and an admin dashboard where HR and management set policy rules and receive severity-graded policy-violation flags (oversight by policy, not a live feed of every conversation) — **not** "the company can never access it." We state this exactly this way in every company conversation.

2. Employee Sovereignty

- Each employee gets a **dedicated instance**; there is no aggregated cross-employee content store.
- A company admin dashboard where HR and management define their own policy rules and receive severity-graded policy-violation flags — oversight by policy, not a live window into every employee conversation or memory.
- Per-employee **Export Everything**; if the license ends, the stack and data are the company's to keep or delete.
- Administrative access is logged; the user-visible **Access Ledger** (Brief §7) is **targeted Q4 2026**.

3. Company Policy Pack

Your AI-use policy is loaded into every employee assistant as a managed file so the assistant **enforces your approved-use rules itself**: it declines disallowed uses, cites the policy, and suggests the allowed path — and raises **severity-graded flags to the company admin dashboard** when a policy is violated. This per-employee policy enforcement and company-defined oversight is unique to the company deployment.

Available on request.

4. What you own vs. what PurposeMapped provides

You own	PurposeMapped provides
AWS account, instances, database, backups, model-provider keys, token spend	Deployment kit (IaC), golden image, provisioning, updates against a pinnable release manifest, support-by-skill (no human reads content), engineering

5. Controls & exit

- Chat surface: your Teams/Slack tenant or a private Matrix — your choice.
- Updates: pull-based against the PurposeMapped release manifest; you can pin versions.
- Support: sanitized failure signatures out, fixes (skills/updates) in — no human in the employee's room.
- Exit: per-employee export; the deployed stack remains in your account if the license ends.

6. Contact

Company deployment inquiries: **support@purposemapped.com** (mark "Company deployment"). We will provide the IaC overview, a security-questionnaire response, and a reference where available.