AI POWER HOUR · TEMPLATE

Our AI use policy

One page your team can read in two minutes. Fill in the blanks, share it Monday, and review it every quarter.

Company: _____ Policy owner: _____ Last reviewed: _____

1. Approved tools

If a tool isn't on this list, ask the policy owner before you use it with company data.

TOOL	PLAN	WHAT IT'S FOR	WHO HAS ACCESS

2. What can go where

- **Public** (website, published docs): any approved tool.
- **Internal** (strategy, financials, our code): approved business-plan tools only.
- **Customer** (names, emails, usage, tickets): only tools with a signed data agreement, or remove names and identifiers first.
- **Regulated** (health, payments, government IDs): not in AI tools unless _____ approves it in writing.

3. Never paste

- Passwords, API keys or access tokens
- Customer data into a personal account
- Our crown jewels: _____

4. A person signs off before AI does any of these

- Sends anything outside the company: emails, posts, messages to customers
- Deletes data
- Spends money
- Touches production systems or live customer data

5. Connecting tools

- Connect only what the job needs, read-only where you can.
- Never connect a work account to a personal AI account.
- New agents start on "ask me every time." Loosen it only after clean runs.

6. Questions and mistakes

- Questions go to the policy owner.
- If something went into the wrong tool, tell the policy owner the same day. No blame; we just need to know.
- This applies to everyone working with our data, contractors included.

AI POWER HOUR · FILLED-IN EXAMPLE

Example: a filled-in AI use policy

The same template, filled in for a made-up 8-person SaaS company.
Copy what fits.

Policy owner: **The CEO** · Last reviewed: **October 2026** · Next review: **January 2027**

1. Approved tools

TOOL	PLAN	WHAT IT'S FOR	WHO HAS ACCESS
ChatGPT	Business (moving from Plus)	Analysis, drafting	Everyone
Claude	Team (moving from Max)	Strategy, writing, research	Everyone
GitHub Copilot	Business	Writing code	Engineering
Gemini in Google Workspace	Business Standard	Email and docs	Everyone
HubSpot (Breeze AI)	Starter, AI model training off	CRM, sales emails	Sales and CEO
Granola	Training off; upgrading	Call notes	CEO, sales

2. What can go where

- Customer exports go into ChatGPT or Claude only after we're on the business plans. Until then, remove names first.
- Regulated data: we don't handle any. If that changes, the CEO decides.

3. Never paste

- API keys, passwords, tokens
- Our pricing engine code
- Real customer data into prototypes. Lovable gets fake data only.

4. A person signs off

- Any email or post going to a customer
- Anything that deletes records in HubSpot or our database
- Any agent with access to production. (Right now, none do.)

5. Connecting tools

- Claude connects to Gmail and Calendar read-only. Nothing connects to production.
- Browser extensions that read what you type need the CEO's OK first.

6. Questions and mistakes

- Ask the CEO. Mistakes reported the same day, no blame.
- Tell customers when a call is recorded by a note-taker.