

AI Usage Policy

How we use AI responsibly across Backpack OS and internally so customer and client data stays protected.

Version: 1.0 · **Last updated:** February 2026 · **Owner:** Security Lead

1. Purpose

To define how Backpack Works uses artificial intelligence and machine-learning tools — both in the Backpack OS product and in internal work — in a way that protects customer, client, and website-visitor data, source code, intellectual property, and confidentiality.

2. Scope

All personnel and contractors who use AI tools for Backpack Works or its clients, the AI features within Backpack OS, and all company, customer, and client data that might be processed by such tools.

3. Product AI (Backpack OS)

- AI features are powered by third-party providers — Anthropic (Claude), OpenAI, Perplexity, and Google (Gemini).
- Where a provider offers the control, we instruct them **not to use customer data to train their generally available foundation models** and configure the service accordingly.
- AI processes only the data needed to perform the requested task. We may use aggregated, anonymized data that does not identify a customer or individual to operate and improve the service.
- AI output is probabilistic and may contain errors; customers control how much autonomy AI has over applied changes and are responsible for reviewing output before publishing.

4. Internal AI use — principles

- **Protect confidential data.** Do not enter confidential client/customer data, personal data, secrets, or credentials into AI tools that may use submitted data to train their models. Prefer enterprise or privacy-respecting configurations.
- **Human accountability.** AI output is assistive, not authoritative; a qualified person reviews AI-generated code, content, and recommendations before it ships.
- **Respect client instructions.** Where a client restricts or prohibits AI use on their engagement, those instructions take precedence.
- **Intellectual property.** Review AI-generated output for IP and licensing concerns before use.

5. Vendors & sub-processors

AI tools that process customer or personal data are evaluated under our Vendor & Third-Party Risk Management Policy and listed as sub-processors where applicable.

6. Enforcement & review

Violations may result in disciplinary action consistent with our Acceptable Use and Information Security policies. This policy is reviewed at least annually and as AI tooling and regulation evolve.