

Vendor & Third-Party Risk Management Policy

How we evaluate and monitor sub-processors and vendors that handle data.

Version: 1.0 · Last updated: December 2025 · Owner: Security Lead

1. Purpose

To manage the security and privacy risks introduced by vendors and sub-processors.

2. Scope

Any third party that processes, stores, or has access to customer, account, website-visitor, or client data — including our infrastructure providers, AI providers, and the analytics and integration services that power Backpack OS.

3. Evaluation

Before engaging a vendor that handles data, we review:

- Their security posture (certifications such as SOC 2 / ISO 27001 where applicable).
- Their privacy practices and data handling, including whether AI providers use inputs to train models.
- Contractual protections, including a data processing agreement where personal data is involved.

4. Sub-processors

We maintain a current, public list of sub-processors at </legal/subprocessors> and provide notice of material changes as required by our agreements.

5. Review

This policy is reviewed at least annually.