

Encryption & Key Management Policy

Standards for encrypting data in transit and at rest and managing keys and secrets.

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

1. Purpose

To define encryption standards that protect data in transit and at rest across Backpack OS and our systems.

2. Standards

- **In transit:** all connections to our applications, APIs, and the customer snippet are served over HTTPS/TLS.
- **At rest:** data in our PostgreSQL database (Supabase) and object storage (Cloudflare R2) is encrypted at rest by our infrastructure providers.
- **Devices:** full-disk encryption on all company workstations.

3. Key & secret management

- API keys and credentials are stored as environment secrets in our deployment platform and are never committed to source control.
- Third-party OAuth and integration tokens are encrypted before storage.
- Internal and company credentials are stored in a dedicated secrets manager (1Password).
- Keys and secrets are rotated on a defined schedule and upon suspected compromise.

4. Review

This policy is reviewed at least annually.