

Secure Software Development Policy

Security practices built into how we design, build, and ship software.

Version: 1.0 · **Last updated:** January 2026 · **Owner:** Engineering Lead

1. Purpose

To ensure security is built into Backpack OS and the software we develop for clients.

2. Scope

All software development performed by Backpack Works, including the platform, the customer snippet, and integrations.

3. Practices

- **Requirements & design:** consider security and privacy needs up front, including tenant isolation and least privilege.
- **Coding:** follow secure coding practices; validate user-supplied values server-side; use parameterized, typed database queries.
- **Application hardening:** configure a Content Security Policy and standard security headers (including clickjacking protection); sanitize content written to customer sites; constrain server-side fetches and integrations to reduce SSRF risk. The customer snippet is bundled and served from our CDN and does not load arbitrary remote code at runtime.
- **Dependencies:** use automated dependency scanning and keep libraries up to date.
- **Code review:** every change is peer-reviewed before merge.
- **Secrets:** never commit secrets; use environment variables and secret stores.
- **Testing:** automated checks run in CI before deployment.
- **Separation:** development, staging, and production are isolated.
- **Security review:** we perform internal reviews across authorization/RLS, secrets and encryption, injection/SSRF/XSS/CSP, and our integration and webhook surfaces.

4. Review

This policy is reviewed at least annually.