

Vulnerability Management Policy

How we find, prioritize, and remediate vulnerabilities.

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

1. Purpose

To identify and remediate vulnerabilities in Backpack OS and the systems we operate.

2. Identification

- Automated dependency and code scanning in CI.
- Platform security advisories and alerts (e.g. Dependabot).
- Internal security reviews across authorization/RLS, secrets, injection/SSRF/XSS/CSP, and integration surfaces.
- Reports submitted through our Responsible Disclosure Policy.

3. Prioritization & remediation targets

Severity	Target remediation
Critical	7 days
High	30 days
Medium	90 days
Low	Best effort / next release

Targets may be adjusted based on exploitability and exposure.

4. Patching

Operating systems, dependencies, and tooling are kept up to date. Critical patches are expedited.

5. Review

This policy is reviewed at least annually.