

Responsible Disclosure Policy

How to report a security vulnerability to Backpack Works.

Last updated: December 2025

Backpack Works values the work of security researchers. If you believe you have found a security vulnerability in Backpack OS (app.backpack.works, cdn.backpack.works), our other systems, or a site or application we operate, we want to hear from you.

How to report

Email **security@backpack.works** with:

- A description of the vulnerability and its potential impact.
- Steps to reproduce, including any proof-of-concept.
- The affected URL, system, or application.

Our commitment

- We will acknowledge your report, typically within five business days.
- We will investigate and keep you informed of our progress.
- We will not pursue legal action against researchers who act in good faith and follow this policy.

Guidelines

Please **do**:

- Give us a reasonable opportunity to remediate before public disclosure.
- Make a good-faith effort to avoid privacy violations, data destruction, and service disruption.

Please **do not**:

- Access, modify, or delete data that is not yours.
- Run automated scans that degrade service availability.
- Engage in social engineering, phishing, or physical attacks against our staff or facilities.

This is a coordinated disclosure program; we do not currently offer a paid bug bounty.