

Network Security Policy

How we segment networks and control traffic to protect systems and data.

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

1. Purpose

To protect Backpack OS and client systems through network segmentation and traffic controls.

2. Scope

The platform (app + snippet/CDN), cloud environments we operate, and remote access to those environments.

3. Controls

- Production, staging, and development environments are logically separated.
- We use our cloud providers' firewalls and security controls to restrict traffic to only what is required.
- Cloudflare serves the customer snippet and assets at the edge, with DNS and DDoS protection.
- Administrative access requires authenticated, least-privilege credentials and is logged.
- Remote access to internal resources uses encrypted connections and MFA.

4. Review

This policy is reviewed at least annually.