

Incident Response Plan

Roles, severity levels, and the steps we follow to detect, contain, and recover from security incidents.

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

1. Purpose

To define how Backpack Works detects, responds to, and recovers from security incidents affecting Backpack OS, our systems, or customer and client data, and how we notify affected customers.

2. Scope

Any event that compromises, or threatens to compromise, the confidentiality, integrity, or availability of platform, customer, account, website-visitor, or client data or systems.

3. Severity levels

- **SEV-1 (Critical):** Confirmed breach of customer or client data, or major platform outage. Immediate response.
- **SEV-2 (High):** Likely security impact or significant degradation.
- **SEV-3 (Low):** Limited or no confirmed impact; investigated during business hours.

4. Response phases

1. **Detect & report.** Anyone can report a concern to security@backpack.works. Incidents are triaged and assigned a severity.
2. **Contain.** Limit the scope — isolate systems, revoke credentials, block access.
3. **Eradicate.** Remove the root cause.
4. **Recover.** Restore systems and validate integrity.
5. **Post-incident review.** Document the timeline, root cause, and corrective actions.

5. Roles

- **Incident Lead** coordinates the response and decisions.
- **Communications owner** manages internal and customer notifications.
- **Engineering** performs containment, eradication, and recovery.

6. Customer notification

If an incident affects customer or client data, we notify affected customers without undue delay after confirming the incident, provide the information reasonably available to support their own obligations, and cooperate with their response.

7. Review & testing

This plan is reviewed at least annually and tested through tabletop exercises.