

# Information Security Policy

The master policy that establishes our commitment to protecting information and governs all other security policies.

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

---

## 1. Purpose

This Information Security Policy establishes Backpack Works' commitment to protecting the confidentiality, integrity, and availability of information — our own and that entrusted to us by our customers and clients. It is the top-level policy of our information security management program and governs all supporting policies.

## 2. Scope

This policy applies to all employees, contractors, and third parties who access Backpack Works systems, customer or client data, or company information. It covers the Backpack OS platform (the dashboard at [app.backpack.works](https://app.backpack.works) and the customer snippet served from [cdn.backpack.works](https://cdn.backpack.works)), the account and website-visitor data we process, our internal systems, and the work we deliver to clients — across all information assets regardless of format or location.

## 3. Policy statements

- **Confidentiality.** Information is classified and protected according to its sensitivity. Access is granted on a least-privilege, need-to-know basis, and customer data is isolated per organization.
- **Integrity.** Information is protected from unauthorized modification through access controls, change management, and code review.
- **Availability.** Systems and data are protected against disruption through managed, redundant infrastructure, backups, and a business continuity plan.
- **Compliance.** We meet applicable legal, regulatory, and contractual obligations, including the GDPR and CCPA/CPRA, and act as a processor on our customers' behalf.
- **Continuous improvement.** We assess risk regularly and improve our controls over time.

## 4. Roles & responsibilities

- **Management** approves this policy, allocates resources, and is accountable for the security program.
- **The Security Lead** maintains policies, coordinates risk assessments, and oversees incident response.

- **All personnel** are responsible for following security policies, completing training, and reporting security concerns to [security@backpack.works](mailto:security@backpack.works).

## 5. Enforcement

Violations of this policy may result in disciplinary action up to and including termination, and may carry legal consequences.

## 6. Review

This policy is reviewed at least annually and after any significant change to the business, platform, technology, or threat landscape.