

Risk Management Policy

How we identify, assess, treat, and monitor information security risks.

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

1. Purpose

To define how Backpack Works identifies, evaluates, treats, and monitors information security risks.

2. Scope

All information assets, systems, processes, and third-party relationships that could affect the security of company or client data.

3. Risk assessment process

1. **Identify** assets, threats, and vulnerabilities.
2. **Analyze** the likelihood and impact of each risk.
3. **Evaluate** risks against our risk acceptance criteria.
4. **Treat** risks by mitigating, transferring, avoiding, or accepting them.
5. **Monitor** risks and the effectiveness of treatments over time.

4. Frequency

A formal risk assessment is performed at least annually and when significant changes occur (new services, major vendors, incidents, or regulatory changes).

5. Risk treatment

Each identified risk is assigned an owner and a treatment plan with target dates. Residual risk that exceeds our acceptance criteria requires management sign-off.

6. Review

This policy is reviewed at least annually.