

Risk Management Policy

How risks to customer data are identified, rated, treated and reviewed.

Version 1.0 · Last reviewed 22 October 2026 · Owner: Security Lead, security@etropo.com · Current version at <https://trust.etropo.com/resources/risk-management-policy>

1. Purpose

Etropo manages security by deciding, on the record, which risks to customer data matter most and what is done about each. This policy sets the method.

2. When

- A full assessment at least once a year.
- A targeted assessment when a new vendor, integration, data class or architectural component is introduced, and after any P0 or P1 incident.

3. Method

1. **Identify** the assets (customer budget data, personal data, credentials and keys, the production platforms, the source code) and the threats to each: unauthorised access, data loss, service loss, vendor failure, insider misuse, supply-chain compromise.
2. **Rate** each risk for likelihood (rare, possible, likely) and impact (minor, serious, severe) and combine them into Low, Medium, High or Critical.
3. **Treat** each risk: mitigate with a control, transfer (insurance, contract), accept with a reason, or avoid by not doing the thing. High and Critical risks are not accepted without the Security Lead's written reasoning.
4. **Assign** an owner and, for mitigations, a date.
5. **Record** the register in the repository and summarise it to the other founders.

4. The register

Each entry has: asset, threat, existing controls, rating, treatment, owner, date, status. The Controls page on this site reflects the treatments that are in place, partial or planned.

5. Standing high-priority risks

Named here so customers can see what the programme is working on:

- **Single-person dependencies.** A small team concentrates production access and knowledge. Treatment: two owners on every system, written procedures, this Trust Center as the record.
- **Limited independent assurance.** Treatment: annual penetration test (most recent October 2026, findings tracked to remediation) and a SOC 2 Type II audit.
- **Database recovery point of 24 hours.** Treatment: evaluate point-in-time recovery; restore from backup tested every year (2025 and 2026).
- **Session replay without text masking in product analytics.** Treatment: enable masking. Done 2026-10-22; text and inputs are masked.
- **AI features that read customer data.** Treatment: provider terms excluding training; same access rules as the user; data sent only on user action.

6. Review

Reviewed annually. Version 1.0, October 2026.

This PDF is a snapshot. The page at <https://trust.etropo.com/resources/risk-management-policy> is the current version.