

Information Security Roles and Responsibilities

The Security Lead, the Infrastructure Lead and everyone else: who is accountable for what, and the current state of coverage.

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

1. Purpose

Security responsibilities at Etropo are assigned to roles so that every control has an owner and every system has someone who can operate it if the owner is unavailable. This document names the roles, what each is accountable for, and the current state of coverage.

2. Roles

Security Lead. The founder responsible for engineering. Accountable for every policy on the Trust Center, for incident response, for access to production systems, for vendor decisions, and for the SOC 2 readiness programme. Reachable at security@etropo.com. Today this is the only person with production access.

Infrastructure Lead. Deputy to the Security Lead and the second owner of production. Access for the role is being set up in October 2026. Once it is complete, the Infrastructure Lead holds owner-level access, with multi-factor authentication, to every system in the asset inventory; runs day-to-day operations (deployments, scheduled jobs, monitoring, backups); deputises as Incident Lead; and can operate the service, respond to an incident and restore from backup from this documentation alone. The single-person dependency named in the Risk Management Policy closes when the Infrastructure Lead holds owner access with multi-factor authentication on every system in the asset inventory and has walked through the Business Continuity Plan.

Engineering. Anyone who writes or deploys code. Responsible for following the Secure Development Policy, for the security of the changes they make, and for reporting suspected incidents. Today engineering and the Security Lead are the same person.

Founders (collectively). Receive the quarterly security report, approve policy exceptions where the Security Lead is conflicted, and are the escalation path for concerns about the Security Lead under the Code of Conduct.

All personnel and contractors. Follow the Code of Conduct, the Acceptable Use Policy and the Confidentiality Agreement.

3. Responsibility matrix

A = accountable (one role), R = does the work, C = consulted, I = informed.

Activity	Security Lead	Infrastructure Lead	Engineering	Founders
Information Security Policy and supporting policies	A, R	C	C	I
Annual risk assessment and register	A, R	C	C	I
Access provisioning, removal and quarterly review	A, R	R	I	I
Production console ownership (Vercel, Supabase, GitHub, Stripe, DNS)	A, R	R		
Secrets and key rotation	A, R	R	I	
Secure development, code review, CI	A		R	
Dependency vulnerabilities and patching	A		R	
Monitoring, alert triage	A, R	R	R	
Incident response: lead	A, R	R (deputy)	R	I
Customer and authority notification after a breach	A, R	C		C
Backups, restore test, BC/DR plan	A, R	R		I
Vendor review, subprocessor list, DPAs	A, R		C	I
Trust Center content and Updates feed	A, R		C	I
Security awareness training completion	A	R	R	R
Code of Conduct and confidentiality acknowledgements	A, R			R

Activity	Security Lead	Infrastructure Lead	Engineering	Founders
Quarterly security report	A, R			I
SOC 2 audit liaison	A, R	C	C	I

4. System owners

Each system in the Asset Inventory names its owner (the Security Lead) and its backup (the Infrastructure Lead).

5. Quarterly report

The Security Lead reports to the founders each quarter on: incidents and their reviews, open vulnerabilities and their age, the result of the access review, changes to the subprocessor list, progress against the readiness backlog, and any policy exception granted.

6. Review

Reviewed annually and whenever a role changes hands. Version 1.0, October 2026.

This PDF is a snapshot. The page at <https://trust.etropo.com/resources/roles-and-responsibilities> is the current version.