

Acceptable Use Policy

Rules for personnel and contractors who use Etropo systems or handle customer data.

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

1. Who this applies to

Everyone who works for Etropo or with it as a contractor and who uses Etropo systems, source code, vendor consoles or customer data.

2. Accounts and credentials

- Use your own account. Never share a login, a token or an API key, and never use someone else's.
- Turn on multi-factor authentication everywhere it is offered. Every production system Etropo uses offers it.
- Use a password manager and a unique password for each system.
- Keep secrets in the system that needs them. Do not paste them into chat, email, documents, tickets or AI assistants.
- Report a lost device or a suspected compromise at once to security@etropo.com.

3. Customer data

- Access customer data only to do the task in front of you: support, a bug, an operation the customer asked for.
- Look at the minimum needed and do not keep copies.
- Do not download customer data to a personal device, removable media or a personal cloud account.
- Do not put customer data into tools that are not on the Subprocessors page.
- Do not discuss a customer's data with anyone who is not entitled to it, inside or outside Etropo.

4. Devices

- Laptops used for Etropo work have full-disk encryption, automatic screen lock, a current operating system and a supported browser.
- Work through the browser and the vendor consoles; do not run production credentials on a personal machine.
- Personal devices may be used for communication and planning tools that hold no customer data.

5. Code and systems

- Follow the Secure Development Policy: branches, pull requests, checks, previews, no secrets in Git.
- Do not disable or bypass a security control (rate limit, Row Level Security, signature check, CI check) to make something work. Raise it instead.
- Do not run tests or scripts against production data outside the confined test organisation.
- Do not install software of unknown origin on a machine that holds production access.

6. Reporting

Report anything that looks wrong, including your own mistakes, immediately and without fear of blame. A quick report is the single most useful thing anyone can do during an incident.

7. Monitoring

Access to production systems is logged by the providers and may be reviewed. There is no expectation of privacy in those logs.

8. Consequences

Breaking this policy can lead to loss of access, termination of employment or contract, and, where the law requires, reporting to authorities.

9. Acknowledgement

Everyone in scope acknowledges this policy on joining and when it changes. Version 1.0, October 2026.