

Human Resource Security Policy

What happens before, during and after a person has access to customer data: agreements, onboarding, training, offboarding.

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

1. Purpose

People are given access to customer data and production systems; this policy sets what happens before, during and after that, for employees, founders and contractors alike. Etropo is a very small company today and the procedures are sized for that, but they apply from the first person onward.

2. Before access

1. **Identity.** Confirm who the person is from an official document before creating any account.
2. **Agreements.** The person signs the Code of Conduct acknowledgement and the Confidentiality Agreement, and reads the Acceptable Use Policy and the Information Security Policy. No access is created until the signed copies are filed.
3. **Role.** The Security Lead decides which systems the role needs, using the least privilege rule in the Access Control Policy, and records the decision on the onboarding checklist.
4. **Background.** Formal background checks are not performed today. References are taken for anyone who will have production access. This is stated here so that no one assumes otherwise.

3. Joining

The onboarding checklist, kept with the person's record, covers:

- individual accounts created on each system the role needs, each with multi-factor authentication turned on at first sign-in;
- a password manager set up;
- the laptop prepared per the Acceptable Use Policy §4 (full-disk encryption, automatic screen lock, current operating system), with a screenshot of the encryption status filed as evidence;
- security awareness training completed within 30 days of joining, certificate filed;
- a walk-through of the Incident Response Plan: how to recognise an incident and whom to tell.

4. During the engagement

- Security awareness training is repeated every year; certificates are filed.
- Access is reviewed every quarter (Access Control Policy §5) and adjusted when a role changes.
- Policy changes are communicated within five working days and re-acknowledged where they change obligations.
- Concerns are raised under the Code of Conduct §3 without fear of disadvantage.

5. Leaving

On the last day, or immediately on an involuntary termination:

- every account on the offboarding checklist (the same list as onboarding, plus anything added since) is removed or disabled, starting with production consoles and source control;
- any shared secret the person could have seen is rotated (Cryptography Policy §6);
- sessions are revoked where the system allows it;
- company devices are returned and wiped; on personal devices used for work, Etropo accounts are removed and the person confirms in writing that no customer data remains;
- the person confirms in writing that confidential information has been returned or destroyed, as the Confidentiality Agreement requires;
- the completed checklist is filed with the date.

6. Contractors

Contractors are treated the same as employees for everything above. Their access is additionally time-limited to the engagement and reviewed at each renewal. A contractor who needs production data access is the exception, not the rule, and is approved by the Security Lead in writing.

7. Records

For each person: identity confirmation, signed acknowledgements, onboarding checklist, training certificates, access review entries, offboarding checklist. Kept for the engagement plus two years.

8. Review

Reviewed annually. Version 1.0, October 2026.