

Security Incident Response Plan

Severity levels, response targets, the steps from detection to post-incident review, and breach notification.

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

1. Purpose

This plan says what Etropo does when something goes wrong with the security or availability of the service: how an incident is recognised, who acts, how fast, what customers are told, and how the lessons are kept.

2. What counts as an incident

Any event that does, or could, compromise the confidentiality, integrity or availability of customer data or of the service. Examples: unauthorised access to an account or system, a vulnerability being exploited, a leaked credential or key, a data loss, a service outage, a vendor incident that affects Etropo's data, or a report from a researcher or customer that turns out to be valid.

3. Severity and response targets

Level	Examples	First response	Updates
P0 Critical	Confirmed unauthorised access to customer data; full outage; exposed encryption key or service credential	Within 15 minutes	Every hour
P1 High	Vulnerability with a public exploit; partial outage affecting several customers; suspected unauthorised access; loss of data integrity	Within 1 hour	Every 4 hours
P2 Medium	Vulnerability needing a patch; degradation for some customers; anomalous authentication failures	Within 4 hours	Daily
P3 Low	Minor issue with no immediate risk; policy non-compliance without data exposure	Within 24 hours	At resolution

The Security Lead assigns the level and can raise it at any point.

4. Roles

- **Incident Lead.** The Security Lead, or the first engineer to respond until the Security Lead takes over. Decides, coordinates and communicates.
- **Responders.** Engineers who investigate and fix.
- **Communications.** The Incident Lead, with the other founders for customer and public statements.

5. Detection

Incidents are detected through:

- Sentry error alerts to the engineering Slack channel;
- Vercel and Supabase status and alerting;
- audit tables for integration syncs, token operations and webhook deliveries;
- rate-limit rejections on authentication endpoints;
- vendor security notifications;
- reports to security@etropo.com from customers and researchers.

Anyone who suspects an incident reports it at once to the Security Lead. There is no penalty for a false alarm.

6. Procedure

Triage. Confirm the event, assign a severity, open an incident record (a Linear issue tagged `incident`) with a timeline that is kept current.

Contain. Stop the harm before understanding all of it: revoke the affected credentials, tokens or sessions; rotate exposed secrets in Vercel; disable the affected integration or feature; roll back the deployment if a change caused it; block abusive sources through rate limiting.

Investigate. Preserve logs and evidence before changing anything further. Establish the root cause, the window, the systems touched, and which customers and what data were affected.

Eradicate. Fix the cause: patch, reconfigure, remove unauthorised access, and verify the fix in preview before deploying.

Recover. Restore the service, from backup if needed, following the Business Continuity Plan. Watch for recurrence for at least 24 hours.

Close. Record the final timeline, impact and actions. Hold a post-incident review within 7 days for every P0 and P1.

7. Communication

Internal. The other founders are told immediately for P0 and P1.

Customers. When customer data was or may have been accessed, altered or lost, the affected customers are told without undue delay, in plain language, with: what happened, what data was involved, what Etropo has done, what the customer should do, and whom to contact. Notification is by email to the organisation's admins.

Authorities. Where the GDPR requires it, the competent supervisory authority is notified within 72 hours of Etropo becoming aware of a personal data breach. Customers for whom Etropo acts as a processor are told in time to meet their own obligations.

Public. A status note is published on the Updates page of this site for incidents that affected several customers.

8. Post-incident review

Every P0 and P1 gets a written review within 7 days that covers the timeline, root cause, what worked, what did not, and the actions taken to prevent recurrence, each with an owner and a date. Reviews are kept and summarised to customers on request. Policies and controls are updated when the review calls for it.

9. Exercising the plan

The plan is walked through once a year in a tabletop exercise against a realistic scenario (for example a leaked service key, or a Supabase regional outage), and the outcome is recorded. The first exercise is scheduled before the SOC 2 observation period.

10. Review

Reviewed annually and after every P0 or P1. Version 1.0, October 2026.