

Transparency by Default

Transparency by Default

Adapted from GitLab's "Transparency by Default" for Security.

Openness is one of NFE's values. In security, being open about how we work, what went wrong and what we changed makes the whole team stronger. Hiding incidents means repeating them.

What we share openly (inside NFE, in this Library)

- Our security policies and how-tos (this book).
- Incident reports once the incident is closed: timeline, root cause, lessons and actions.
- Results of access reviews and security checks (summarised).

What we keep confidential

- Passwords, keys, tokens and anything that would help an attacker right now (unpatched weaknesses, exact firewall rules). These go in the password manager or a restricted folder.
- Personal data of customers, team members and partners.
- Details of an incident **while it is still being handled**, shared on a need-to-know basis.
- Partner or funder information shared with us in confidence.

Writing incident reports

- **Blameless:** describe what happened and why the system allowed it, not who to blame.
- Remove secrets, and anyone's personal data beyond what's needed.
- Include what is **still unknown**, and clear actions with owners.

Sharing outside NFE

Security information goes outside NFE (to customers, funders, the public) only with approval from the Security DRI and a director. If customer data was exposed, we may be legally required to notify the people affected.

Revision #1

Created 2026-10-20 23:51:53 UTC by MCP Server

Updated 2026-10-21 00:02:17 UTC by MCP Server