

Security at NFE

Security at NFE

“ This book is adapted from the [Security section of the GitLab Handbook](#) (CC BY-SA 4.0), scaled down for a small team running self-hosted tools and field energy systems. See *About this book* at the bottom.

Vision and mission

Vision: keep the people, communities and partners who depend on NFE safe. That covers our customers' power, their data and our own systems, and we do it openly.

Mission: let the team build and ship quickly on tools and systems we trust. We follow five operating principles, borrowed from GitLab.

1. **Help the business succeed**

- Prefer boring, step-by-step fixes that lower risk.
- Find ways to say yes.
- Understand the goal before recommending a solution.
- Use our own tools first (Nextcloud, the Library, Plane).

2. **Run efficiently**

- Technical controls beat written rules. Example: enforcing 2FA beats asking people to be careful.
- Automate before adding manual checks.
- Prefer reusable solutions over one-offs.

3. **Be transparent**

- Document incidents and decisions here in the Library.
- Protect what is confidential (customer data, credentials, partner information).
- Use plain language and avoid security jargon.

4. **Reduce risk**

- Secure by default.
- Prevention beats detection.
- Fix root causes, not symptoms.
- Make sure we can see what happens through logs, alerts and inventories.

5. **Work together**

- Solve shared problems once, for everyone.
- Help each other succeed. Security is everyone's job.

We also use AI tools (such as Claude) to automate checks and investigations, with the same care for credentials and data as any other tool.

How security is organised at NFE

GitLab splits security into four departments. NFE is small, so each area has a **DRI** (directly responsible individual) instead of a team. See [Directly Responsible Individuals](#).

Area	GitLab equivalent	What it covers at NFE	DRI
Secure the product	Product Security	Meters, inverters, OpenEMS / Raspberry Pi edge devices, the inverter monitor, Modbus/MQTT, firmware and code we write	Tech lead
Protect the company	Security Operations	Incident response, monitoring, log review, abuse of our accounts	Security DRI (currently Aaron)
Protect the organisation	Corporate Security	Nextcloud, mail (Roundcube, SMTP), BookStack, ERPNext, accounts, 2FA, app passwords, laptops and phones	Security DRI + Federated Computer (our host)
Assure partners	Security Assurance	Policies in this book, answering partner and funder security questionnaires, access reviews	Security DRI

Report an incident

If you think something is wrong, **report it now**. Don't wait until you're sure. Examples:

- a lost or stolen laptop or phone;
- a password or app password that may have leaked (typed into a strange page, sent in chat, found in a file);
- a device that may be infected, or that is acting strangely;
- bounce messages for mail you didn't send;
- customer, partner or financial data exposed by mistake.

How to report: see [Reporting a Security Incident](#).

What's in this book

- **Incident Response:** reporting, severity matrix, response guide, leaked credentials, ransomware.
- **Team Member Security:** passwords, accounts and 2FA, email and phishing, devices and networks, onboarding/offboarding.
- **Policies and Standards:** access management, audit logging, encryption, transparency.
- **Product Security:** securing meters, inverters and edge devices.
- **Incident Reports:** what happened in past incidents and what we changed.

About this book

Structure and much of the wording are adapted from the GitLab Handbook (handbook.gitlab.com/handbook/security), licensed CC BY-SA 4.0. Changes: scaled to NFE's size, tools and systems. This book is shared under the same licence.

Please improve it. Edit any page, or ask Claude to update it using the NFE Library skill.

Revision #1

Created 2026-10-20 23:47:12 UTC by MCP Server

Updated 2026-10-21 00:02:04 UTC by MCP Server