

Security

How NFE keeps its people, systems, customers and data safe: incident response, team security, policies and incident reports.

- [Security at NFE](#)
- [Incident Response](#)
 - [Reporting a Security Incident](#)
 - [Security Incident Severity Matrix](#)
 - [Security Incident Response Guide](#)
 - [Leaked Credentials Runbook](#)
 - [Responding to Ransomware](#)
- [Team Member Security](#)
 - [Password Guidelines](#)
 - [Accounts, 2FA and App Passwords](#)
 - [Email Security and Phishing](#)
 - [Device and Network Security](#)
 - [Onboarding and Offboarding Access](#)
- [Policies and Standards](#)
 - [Access Management Policy](#)
 - [Audit Logging Policy](#)
 - [Encryption Standard](#)
 - [Transparency by Default](#)
- [Incident Reports](#)
 - [2026 Mailbox Compromises: spam sent from NFE accounts](#)
- [Product Security](#)
 - [Field Device and Code Security Baseline](#)

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.

Incident Response

How to report a security incident, how we classify severity, and how we respond. Adapted from GitLab's SIRT pages.

Reporting a Security Incident

Reporting a Security Incident

Adapted from GitLab's "Engaging the Security Engineer On-Call".

If in doubt, report it. A false alarm costs a few minutes. An unreported compromise cost us weeks in 2026 (see Incident Reports).

What counts as an incident

- A lost or stolen laptop, phone or USB drive that holds NFE data or saved passwords.
- **Leaked credentials:** your password or an app password typed into a suspicious page, pasted in chat or email, committed to code, or seen by someone else.
- A device that may be infected: pop-ups, unknown apps, antivirus alerts, browser extensions you didn't install.
- **Bounces or replies for mail you never sent.** This is the sign that someone is sending as you.
- Logins, devices or app passwords you don't recognise (Nextcloud → Personal settings → Security).
- Customer, partner or financial data shared with the wrong people.
- Anything strange on field equipment: meters, inverters, Raspberry Pi/OpenEMS devices changing settings on their own, unknown SSH logins.

How to report

1. **Urgent** (you may be compromised right now, or customer power or data is affected):
 - Message the Security DRI directly in Nextcloud Talk **and** phone or WhatsApp them.
 - If you can't reach Talk or your NFE account (e.g. your password was changed), use your personal email or phone. Don't wait.
2. **Not urgent** (a suspicious email you didn't click, a question):
 - Post in the team Talk chat or message the Security DRI. Expect an answer within one working day.

Include:

- what you saw, and when (with timezone);
- which account, device or system;
- what you already did (clicked a link, entered a password, replied);
- screenshots or the original email. **Forward suspicious mail as an attachment; don't just describe it.**

Phishing

- **Didn't engage** (no click, no reply): report it, then delete it or move it to Junk.
- **Engaged** (clicked a link, entered a password, opened an attachment, replied, sent money or gift cards): treat it as **urgent**. Change your password straight away from a device you trust, then report.

What happens next

The Security DRI triages the report, sets a severity using the [severity matrix](#), and follows the [incident response guide](#). You may be asked to stay available to answer questions in the first hour.

Security Incident Severity Matrix

Security Incident Severity Matrix

Adapted from GitLab's Security Incident Severity Matrix.

Purpose

A standard way to classify how serious a security incident is. Severity decides how fast we respond, who gets involved and who we tell. It is set during the first triage.

Matrix

Severity	Impact	NFE response	Examples
S1 Critical	Customers lose power or their data is exposed, or severe damage to NFE (money, reputation, funder trust)	Drop everything. All available team members help. Updates at least every few hours.	Confirmed breach of customer or financial data. An attacker controls an admin account (Nextcloud <code>admins</code> , server root, ERPNext admin). Remote control of meters or inverters at a site. Ransomware on a shared system.
S2 High	Significant disruption for customers or the team, or likely damage to NFE	Named responder; same-day action; daily updates	A mailbox used to send spam (Mar–Apr 2026, Aug–Sep 2026). Suspected unauthorised access to Nextcloud or mail. Malware on a team laptop. Our mail relay IP listed on Spamhaus.
S3 Medium	Moderate impact; work is hampered	Handle within the week alongside normal work	A phishing link clicked but no password entered. Weak config found on a field device with no sign of abuse. Infected device that held no NFE credentials.

Severity	Impact	NFE response	Examples
S4 Low	Minimal impact; workaround available	Normal process / backlog	A policy slip with no sensitive data involved (e.g. a password in a private note, now changed). Phishing reported without engagement.

Things to weigh

- **Confidentiality, integrity, availability:** which of these are affected? The more, the higher the severity.
- **Affected surface:** customer sites and meters → shared servers (Nextcloud, mail, ERPNext, BookStack) → one account → one device.
- **Exploitability:** does it need one command, some effort, or rare conditions?
- **Visibility:** can everyone see it, people with specific access, or only you?
- **Privilege:** members of the Nextcloud `admins` group, server root and field-device admin accounts raise severity by one level.

When unsure, choose the **higher** severity. You can lower it after investigation.

Security Incident Response Guide

Security Incident Response Guide

Adapted from GitLab's Security Incident Response Guide (SIRT).

Scope

Any event that may harm NFE, our customers, partners or team members, or that breaks our security or acceptable-use policies. That includes incidents at providers we depend on, such as Federated Computer (hosting and mail relays). The Security DRI decides whether an event becomes an incident. Reports can come from anyone, inside or outside NFE.

Roles

Role	Responsibility
Team members	Report quickly; follow instructions; preserve evidence (don't delete suspicious mail or files)
Security DRI (incident lead)	Triage, set severity, coordinate the response, keep the incident record, write the report
System owners	Help contain and recover their system (e.g. Federated Computer for mail/LDAP, tech lead for field devices)

Phases

1. **Detection:** a team member, an alert, a partner or a bounce wave tells us something is wrong.

2. **Analysis:** confirm it's real. Set severity with the [matrix](#). Record the start time, systems and accounts involved.
3. **Containment:** stop it spreading.
 - Change the affected passwords.
 - Revoke app passwords and sessions.
 - Disable the account if needed.
 - Isolate the device or take it off the network.
 - Ask the host to pause outbound mail for the account.
4. **Eradication:** remove the attacker's access.
 - Check for forwarding rules, Sieve filters, aliases and new app passwords.
 - Check for unknown SSH keys and installed software.
 - Fix the weakness that let them in.
5. **Recovery:** restore normal operation, add monitoring for a repeat, and confirm with the affected person.
6. **Post-incident:**
 - Hold a short retrospective.
 - Write it up in **Incident Reports** (timeline, root cause, evidence, what's still unknown, actions).
 - Turn the actions into Plane tasks with owners.

Leaked credentials

When a secret has leaked (password, app password, API key, SSH key, token), **revoke it immediately**, even before we know the full impact. A broken integration is cheaper than an abused credential. Then tell the owners of anything that used it. See [Leaked Credentials Runbook](#).

Evidence

- Keep originals. Move suspicious mail and bounces into a folder; don't trash them.
- Note what you did and when (UTC).
- Ask providers for logs early, because logs rotate. For mail, ask Federated Computer for Postfix SASL, Dovecot and Roundcube login logs.
- **Never paste a leaked password into a report, chat or ticket.** Write "old password (redacted)".

Confidentiality

Incident details often include personal or customer data, so share them only with the people who need them. Once the incident is closed, the report is shared in the Library with sensitive details removed. See [Transparency by Default](#).

Leaked Credentials Runbook

Leaked Credentials Runbook

Use this when an NFE password, app password, API key or SSH key may be known to someone else. It was written after the 2026 mailbox compromises.

“ **Important:** at NFE, **one LDAP password** unlocks Nextcloud, IMAP/SMTP mail and Roundcube webmail. A leaked mail password is a leaked Nextcloud password, and for members of `admins`, a leaked admin password.

1. Contain (first hour)

1. **Change the password** from a device you trust. Use a new, random, unique password from a password manager.
2. **Nextcloud → Personal settings → Security → Devices & sessions:**
 - revoke every session and app password you don't recognise;
 - when in doubt, revoke them all and re-create the ones you need.
3. **Mail settings:** check for anything you didn't create.
 - Nextcloud Mail → Account settings → Filters and Autoresponder.
 - Roundcube → Settings → Filters / Identities / Responses.
 - Look for forwarding, redirect or vacation rules and extra identities.
4. Ask the Security DRI to ask **Federated Computer** to:
 - confirm the account is no longer sending;
 - pause outbound mail for it if it still is;
 - share SASL/Roundcube login logs (source IPs, times).

2. Find how it leaked

- **Reuse:** was the same password used anywhere else? Check haveibeenpwned.com for your NFE address.
- **Infostealer:** were passwords saved in a browser or mail app on a device that could be infected? Scan it, and change every password saved on that device.

- **Phishing:** did you type the password into a page reached from an email link?
- **Exposure:** was it pasted in chat, email, a file, a screenshot or code?

3. Clean up

- Delete (with the Security DRI's agreement) any mail or file that contains the old password, e.g. "SMTP checker" bounces.
- Rotate anything that was shared alongside it (shared accounts, API keys in the same note).
- Update every legitimate device with its own **app password**. See [Accounts, 2FA and App Passwords](#).

4. Record

Open an incident record and, when closed, add a report to **Incident Reports**.

Responding to Ransomware

Responding to Ransomware

Adapted from GitLab's "Responding to Ransomware".

Ransomware encrypts files and demands payment. It can arrive through a phishing attachment, a compromised account, or an exposed device or server. **NFE's position: we restore from backups rather than pay a ransom.**

First steps

1. **Disconnect the affected device from the network** (Wi-Fi off, cable out). Don't switch it off: memory can hold useful evidence.
2. **Stop Nextcloud sync** on that device. Encrypted files can sync to the server and to colleagues. Pause the desktop client, or ask the Security DRI to disable the account.
3. Report as **S1** ([Reporting a Security Incident](#)).
4. Don't contact the attackers and don't delete the ransom note. Take photos or screenshots.

Recovery

- **Nextcloud** keeps file versions and a trash bin. Damaged files can usually be rolled back per file, or in bulk by an admin.
- Server-side backups are held by **Federated Computer**. Ask them for a restore point from before the infection.
- Field devices (Raspberry Pi / OpenEMS): re-image from a known-good image and re-apply configuration from version control. Never restore from the infected card.
- Reinstall the affected laptop before it rejoins the network. Change every password that was saved on it.

Who to involve

- **Security DRI:** leads the response.
- **Federated Computer:** server backups, mail, LDAP.

- **Tech lead:** field devices and customer sites, if affected.
- **Board / directors:** for S1. They decide on external communication, including telling customers or funders if their data was involved, which may be legally required.

Prepare now

- Check that backups exist and **test a restore** at least once a year.
- Keep operating systems and apps updated; see [Device and Network Security](#).

Team Member Security

What every NFE team member does to keep accounts, email and devices safe. Adapted from GitLab's Corporate Security pages.

Password Guidelines

Password Guidelines

Adapted from GitLab's Password Guidelines, which follow NIST SP 800-63B.

Passwords are still the main lock on most NFE systems. Our NFE password (LDAP) opens **Nextcloud, mail (IMAP/SMTP) and Roundcube webmail**. Treat it as the key to everything.

The rules

1. **Use a password manager.** Remember one strong master password and let the manager generate the rest. Until NFE picks a team manager, use a reputable one such as Bitwarden or KeePassXC (proposal; to be decided).
2. **Every password is unique.** Never reuse your NFE password anywhere else, not even a variation of it. Reuse is the most common way accounts get taken over, through leaked "combo lists" from other sites.
3. **Long beats complex.** At least 16 characters, generated, or a passphrase of 5+ random words. No forced rotation, but **change it at once if it may have leaked**.
4. **Don't let browsers save your NFE password.** Infostealer malware harvests browser-saved passwords. Use the password manager instead.
5. **Never share passwords** by email, chat, Talk, Deck cards, screenshots or Library pages, and that includes login email addresses together with passwords. Share credentials through the password manager's sharing feature or a Nextcloud share with a password and an expiry date, and delete it after use.
6. **Use app passwords for devices and tools** (phone mail, desktop sync, scripts, Claude skills). Never use your main password there. See [Accounts, 2FA and App Passwords](#).
7. **Security questions:** don't answer truthfully. Store a random answer in the password manager.
8. **Check for breaches:** turn on your manager's breach alerts (e.g. Bitwarden reports, 1Password Watchtower). Check your NFE address at haveibeenpwned.com.

Master password

- Keep it secret, including from admins and the Security DRI. If anyone else learns it, change it.
- Don't store it in the password manager itself or in a browser. Write the recovery/emergency kit down and keep it somewhere physically safe.

Field and shared device passwords

Default passwords on inverters, meters, routers and Raspberry Pis (e.g. `admin/admin`) **must be changed before a device goes to a site**. Store device credentials in a shared vault, never in Library pages or code. See [Field Device and Code Security Baseline](#).

Accounts, 2FA and App Passwords

Accounts, 2FA and App Passwords

Adapted from GitLab's identity and access guidance, for NFE's Nextcloud + LDAP setup.

How NFE accounts work

System	How you log in	Notes
Nextcloud (files, Talk, Deck, Mail app, Calendar)	NFE username + LDAP password	Supports 2FA (TOTP) and app passwords
Mail: IMAP/SMTP (phone and desktop mail apps)	full email address + LDAP password	No 2FA. A stolen password can send mail directly.
Roundcube webmail (roundcube.nearlyfreeenergy.com)	email + LDAP password	Public login page, no 2FA today
BookStack (this Library)	own login	
ERPNext, Plane, others	own logins	Turn on 2FA wherever offered

Because mail and webmail accept the bare LDAP password, **2FA in Nextcloud alone does not stop someone with your password from sending mail as you.** That is exactly what happened in 2026.

What every team member does

1. **Turn on 2FA in Authelia**, NFE's login screen for all Core apps. Follow **Setting up 2FA (current approach)** below. *Required for every NFE account.*
2. **Use Nextcloud Mail or Roundcube in the browser** instead of saving your LDAP password in phone or desktop mail apps where possible.
3. **One app password per device or tool:**

- Create it in Nextcloud → Personal settings → Security → Devices & sessions → *Create new app password*.
 - Name it after the device or tool (`aaron-phone-mail` , `claude-api` , `dansturn-laptop-sync`).
 - Revoke it when the device is lost, replaced or no longer used.
4. **Review Devices & sessions monthly.** Revoke anything you don't recognise and report it.
 5. **Admins:** use your admin rights only when you need them. The Security DRI reviews `admins` membership every quarter.

Setting up 2FA (current approach)

Every NFE account must have two-factor authentication (2FA). Our apps sign in through **Authelia**, the NFE login screen at `authelia.nearlyfreeenergy.com`, so you set 2FA up there once and it covers every app that requires it.

“ **Important: add the key using the URI, not the QR code.** At the moment our Authelia only accepts codes from authenticator apps that were set up with the full `otpauth://` link (the URI). Scanning the QR code or copying the "Secret" into Google Authenticator or Duo produces codes that Authelia rejects: the field turns red, even with a fresh code. We've asked Federated Computer to switch Authelia to standard settings so any app works. This page will be updated when that's done.

What you need: your NFE login, access to your NFE email (for a confirmation code), and an authenticator that accepts a URI. We recommend **Vaultwarden/Bitwarden**, our password manager. Aegis and 2FAS also work.

Steps

1. Go to **authelia.nearlyfreeenergy.com** and sign in with your NFE username and password.
2. Open **Settings → Two-Factor Authentication** and choose to add a **One-Time Password**.
3. Authelia emails you a one-time code to confirm it's you. Enter it in the browser. Never share this code with anyone, including IT support.
4. On the registration screen, **copy the URI** (the link starting with `otpauth://`). Don't scan the QR code and don't copy the "Secret".
5. In Vaultwarden/Bitwarden, create or edit a login item called "NFE Authelia", paste the URI into the **Authenticator key (TOTP)** field, and save. A 6-digit code now appears on the item.

6. Type the current code into Authelia and confirm. Wait for a new code if one was already used or is about to expire.
7. Store any backup or recovery details in your password manager, never in email, chat or this Library.

Afterwards

- Authelia emails you whenever a 2FA method is added or removed. If you get one of these emails and didn't make the change, report it immediately (see [Reporting a Security Incident](#)).
- If you get locked out, contact the Security DRI, who will ask Federated Computer to reset your 2FA. Don't turn 2FA off yourself to get around a problem.
- Federated's walkthrough video of the URI method is saved in our support thread with them. Ask Aaron for a copy.

Last reviewed: 21 October 2026, Aaron Tushabe.

Planned improvements (Security DRI + Federated Computer)

- 2FA for Roundcube (e.g. `twofactor_gauthenticator`), or retire Roundcube in favour of Nextcloud Mail.
- Per-user outbound mail rate limits and alerts on unusual sending volume.
- Rate-limiting and blocking of repeated failed logins (fail2ban) on SMTP/IMAP/Roundcube.
- Investigate app-password-only access for IMAP/SMTP, so the main password never sits in a mail app.

Email Security and Phishing

Email Security and Phishing

Adapted from GitLab's Phishing Program and Email Security Standards.

Email is the most common way into an organisation: phishing pages steal passwords, attachments install malware, and fake invoices or "urgent" requests trick people into paying.

How to spot phishing

- **Urgency or fear:** "your mailbox will be deleted today", "invoice overdue", "account suspended".
- **Login links:** "verify your account", "storage full", "shared document". NFE systems never ask you to log in from an email link. Open nextcloud.nearlyfreeenergy.com yourself.
- **Mismatched sender:** a display name that says "Nextcloud Admin" but a strange address, or a Reply-To that differs from From.
- **Unexpected attachments:** `.html`, `.htm`, `.zip`, `.iso`, `.exe`, Office files asking to "enable content".
- **Money or gift-card requests,** even from a colleague's name. Confirm by phone or Talk.
- **Grant, loan and "funding" offers** that ask for fees or personal details.

What to do

You...	Do this
Got a suspicious email, didn't interact	Forward it as an attachment to the Security DRI or post in Talk, then move it to Junk
Clicked a link but entered nothing	Report it (S3). Close the tab. Run a malware scan
Entered your password, opened an attachment or replied	Urgent: change your password from a trusted device, then follow the Leaked Credentials Runbook
See bounces for mail you didn't send	Urgent: your account is probably sending spam. Report immediately

Domain protections (nearlyfreeenergy.com)

Checked October 2026:

- **SPF:** `-all` (strict), covering our server and the Federated Computer relays. Has some duplicate entries to tidy.
- **DKIM:** selector `mail`, published.
- **DMARC:** `p=quarantine; sp=none`, with reports to admin@. *Target:* `p=reject; sp=reject` once reports look clean.

These stop other people **forging** our domain. They don't stop someone who has a real NFE password: that mail is genuinely signed. So account protection (2FA, unique passwords, rate limits) matters most.

Training

Phishing awareness is part of onboarding. The Security DRI may run occasional practice phishing emails. If you report them, great; if you click, you'll get a short refresher, with no blame.

Device and Network Security

Device and Network Security

Adapted from GitLab's device standards and "Isolating your work laptop from other devices in your home".

Your laptop and phone hold your NFE sessions, synced files and often saved passwords. An infected device leaks everything on it. **Infostealer malware is a likely way our 2026 mail passwords leaked.**

Laptops and desktops

- **Keep it updated:** turn on automatic OS and browser updates and restart when asked.
- **Full-disk encryption on:** FileVault (macOS), BitLocker or Device Encryption (Windows), LUKS (Linux).
- **Screen lock** after 5 minutes or less, with a password, PIN or biometrics.
- **Malware protection:** Windows Defender is fine on Windows. Run a scan after anything suspicious.
- **Install software only from official sources.** No cracked software, "free" game cheats or unknown browser extensions. These are the main way infostealers spread.
- **Separate user accounts** if family members share the computer. Ideally, keep a separate work device.
- **Don't save the NFE password in the browser.** Use a password manager.

Phones

- Screen lock and automatic updates on.
- Install apps from the official app store only.
- Use an **app password** for mail and Nextcloud apps, never your main password.
- If the phone is lost, revoke its app passwords and sessions straight away (Nextcloud → Devices & sessions) and report it.

Networks

- **Home network:** change the router's default admin password, use WPA2/WPA3, and keep the router firmware updated. Put smart-home and IoT devices on a guest network if possible, separate from your work laptop.
- **Public Wi-Fi:** NFE services use HTTPS, so normal use is fine. Avoid admin work (servers, field devices) on public Wi-Fi unless you're on a VPN or tunnel (Tailscale/WireGuard).
- **Never expose field devices** (Raspberry Pi, inverter or meter interfaces, Modbus) directly to the internet. Use a VPN or tunnel.

USB drives

Encrypt drives that carry NFE data. Don't plug in drives you found or were given unexpectedly.

Onboarding and Offboarding Access

Onboarding and Offboarding Access

Adapted from GitLab's CorpSec Onboarding/Offboarding Services.

Onboarding checklist (new team member)

- ☐ NFE account created in LDAP/Nextcloud, with only the groups the role needs (**not** `admins` by default).
- ☐ The new member sets their own password (generated, unique) and turns on **Nextcloud 2FA** in week one.
- ☐ Password manager set up; see [Password Guidelines](#).
- ☐ App passwords created per device, not the main password.
- ☐ Reads this Security book, especially *Reporting a Security Incident* and *Email Security and Phishing*.
- ☐ Access to other systems (ERPNext, Plane, BookStack, field devices) requested and recorded by the onboarding buddy.

Offboarding checklist (leaving or role change), same day

- ☐ Disable the LDAP account (this blocks Nextcloud, mail and Roundcube).
- ☐ Revoke all Nextcloud sessions and app passwords.

- ☐ Remove the person from `admins` and other privileged groups.
- ☐ Remove their SSH keys from servers and field devices. Rotate any shared device or service credentials they knew.
- ☐ Transfer ownership of files, Deck boards, calendars and Library pages they own.
- ☐ Decide on mail: forward to a teammate for a set period or set an auto-reply. Don't leave an active, unwatched mailbox.
- ☐ Recover NFE equipment and wipe it.

For role changes, remove access that the new role doesn't need. **Access is reviewed every quarter;** see [Access Management Policy](#).

Policies and Standards

Access management, audit logging, encryption, and transparency. Adapted from GitLab's Security and Technology Policies.

Access Management Policy

Access Management Policy

Adapted from GitLab's Access Management Policy.

Purpose and scope

Make sure only the right people have access to NFE systems and data, with no more access than they need. This covers Nextcloud, mail, LDAP, BookStack, ERPNext, Plane, servers, cloud and DNS accounts, and field devices (meters, inverters, edge computers).

Principles

- **Least privilege:** give the minimum access needed for the role. Admin rights are the exception, not the default.
- **Need to know:** sensitive data (customer, financial, personal, credentials) is shared only with people whose work requires it.
- **Unique accounts:** one person, one account. No shared logins except documented service accounts.
- **Strong authentication:** 2FA wherever the system supports it. **Required for admins.**
- **Service accounts and API keys** (e.g. `MCP Server`, `claude-api`, `cli`) each have an owner, a purpose and the narrowest scope possible. They are listed in the access register.

Granting access

The person's lead or the Security DRI approves access, and it is recorded in the access register (a Nextcloud spreadsheet in the Security folder; to be created). Admin access needs approval from the Security DRI.

Reviews

Every **quarter**, the Security DRI reviews:

- members of the Nextcloud `admins` group and other privileged groups;
- every user's app passwords and sessions (each person checks their own; admins check service accounts);
- accounts of people who have left;
- field-device and server SSH keys.

Access that's no longer needed is removed. Each review gets a dated note in the Library.

Removing access

When someone leaves or changes role, access is removed the same day; see [Onboarding and Offboarding Access](#).

Exceptions

Exceptions need written approval from the Security DRI, recorded with a reason and an end date.

Audit Logging Policy

Audit Logging Policy

Adapted from GitLab's Audit Logging Policy.

Why

We can only investigate what we logged. In the 2026 mailbox incidents, the **login and source-IP evidence had already gone** from Nextcloud's activity stream (it kept about 6 months), and mail submission headers don't record the sender's IP. This policy closes that gap.

What must be logged

System	Events	Owner
LDAP / mail (Postfix, Dovecot)	Successful and failed logins with username, source IP and time; messages sent per authenticated user	Federated Computer
Roundcube	Logins (<code>userlogins</code> log) with IP	Federated Computer
Nextcloud	Logins, failed logins, app-password and 2FA changes, admin actions, sharing (the admin_audit app)	Security DRI
BookStack, ERPNext	Logins and admin changes (built-in audit logs)	System owners
Servers and field devices	SSH logins, sudo use, config changes	Tech lead

Retention

Keep security logs for **at least 12 months**, so an incident found months later can still be investigated. Logs must be protected from changes and readable only by admins.

Review and alerts

- Alert when one account sends unusually many messages per hour, or logs in from a new country.
- The Security DRI checks failed-login and sending-volume summaries monthly, and DMARC aggregate reports (sent to admin@) monthly.

Status

As of October 2026, retention and alerting are **not yet confirmed** with Federated Computer. That is an open action from the 2026 incident report.

Encryption Standard

Encryption Standard

Adapted from GitLab's Encryption Policy.

In transit

- Every NFE web service (Nextcloud, BookStack, ERPNext, webmail) uses **HTTPS with TLS 1.2+**. Plain HTTP only redirects to HTTPS.
- Mail clients connect with TLS (IMAPS 993, SMTP submission 587 with STARTTLS or 465). Never with plain-text auth.
- Field devices report over encrypted channels: TLS for MQTT, a VPN or tunnel (WireGuard/Tailscale) for remote admin. Modbus/TCP has no encryption, so it must **stay on local networks** or inside a tunnel.

At rest

- Laptops: full-disk encryption on (FileVault / BitLocker / LUKS).
- Phones: device encryption with a screen lock (the default on modern phones).
- USB drives and backups holding NFE data: encrypted.
- Server disks and backups: encrypted by the host. Confirm with Federated Computer.

Secrets

- Passwords, API keys, tokens and private keys are kept in a password manager or the system's own secret store. **Never** in Library pages, Deck cards, chat, email, code repositories or unencrypted files.
- Rotate a secret straight away if it may have been exposed; see [Leaked Credentials Runbook](#).
- Use modern algorithms: RSA $\geq$ 2048 or Ed25519 for keys; never MD5 or SHA-1 for security purposes.

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.

Incident Reports

Write-ups of past security incidents: what happened, root cause, and what we changed. Internal only.

2026 Mailbox Compromises: spam sent from NFE accounts

Incident report: spam sent from aaron.tushabe@nearlyfreeenergy.com (31 Mar – 1 Apr 2026)

*Prepared 20 Oct 2026 · read-only investigation (nothing was changed, deleted or sent) · **Status:** open, severity S2 (see the [severity matrix](#))*

Summary

The spam was **real, authenticated mail sent through NFE's own mail server**, not spoofing or backscatter. Someone had Aaron's **mailbox password** (the LDAP password shared by IMAP/SMTP, Roundcube webmail and Nextcloud). Several separate spam operators used it during a **~6-hour window, 31 Mar 2026 18:52 UTC → 1 Apr 01:11 UTC**:

- some logged in to **Roundcube webmail** (webmail.nearlyfreeenergy.com) and sent Bcc blasts of 99 recipients each;
- others used **SMTP AUTH** on smtp.nearlyfreeenergy.com:587/465 with bulk-mailing tools.

The bounces that came back on 1–9 April were delivery failures and retries for mail submitted in that window. **Nothing was sent after 01:11 UTC on 1 Apr.**

The password most likely came from a **leaked credential list ("combo list")**: the attackers' own tool messages say "PydroidCH SMTP Cracker EMAIL:PASS". The leak itself is still unexplained. Possible sources: an infostealer on a device, a phishing page, or the same password used on another site.

A **second, separate compromise** hit **dansturn.kimbowa@** from May to 3 Sep 2026. It used SMTP only, a different spam tool and German-language phishing/dating spam (see below). The common weakness: NFE's mail server accepts a bare password for SMTP submission, with no 2FA

and no per-user sending limits.

Evidence

Finding	Evidence
Sent through NFE's server, authenticated	Every returned original is DKIM-signed <code>d=nearlyfreeenergy.com s=mail</code> (only NFE's server holds that key), has envelope sender <code>aaron.tushabe@...</code> , and passed SPF/DKIM/DMARC at Gmail. Bounces come from NFE's own outbound relays (fi-relay / de-relay.federatedcomputer.com).
Password was harvested and tested by an SMTP checker	Messages from the account to attacker addresses: "You get a new smtp", "HIT [] smtp.nearlyfreeenergy.com", "SMTP Checker Test - PydroidCH SMTP Cracker EMAIL:PASS", plus "Jerry Rivera" (a host port user pass line). They contain the full old password in clear text , with the login given as the full email address.
Roundcube webmail was used	"Loan Offer" (Samuel Braandon) and "US Department of the Treasury" (Danny Alba) carry Roundcube's fingerprint: <code>X-Sender</code> , <code>Mail-Reply-To</code> , <code>format=flowed</code> , md5 Message-IDs. 41 copies are in Sent (5-99 Bcc each, 3,965 recipients) and ~42 attacker drafts are in Drafts (31 Mar 19:24-00:16 UTC). Roundcube saves both automatically. Roundcube 1.7.x is publicly reachable at <code>webmail.nearlyfreeenergy.com</code> .
SMTP AUTH with a bulk mailer was also used	The "Emily Portney" campaigns ("I need your quick response", "Please get back to me") went one recipient per message, with Message-IDs in <code>YYYYMMDDhhmmss.HEX@domain</code> format, and were never saved to Sent.
Multiple operators	Different personas, reply-to addresses and sender timezones (-07:00, -04:00, +03:00, +13:00), and "hit" notices sent to five different attacker mailboxes. This fits a credential that was sold or shared.
Not a Nextcloud Mail send	The Nextcloud Mail outbox is not involved, and none of the originals have Nextcloud Mail headers.
No persistence left in mail settings	The active Sieve script only holds Aaron's three filing rules: no redirect, forward or vacation. No aliases.

Timeline (UTC)

Time	Event
31 Mar 18:52	First spam submitted ("From Patricia E. Harri...", "Patricia Bloomberg Foundation" persona)

Time	Event
18:54 → 22:04	"Loan Offer" Bcc blasts via Roundcube (~570 bounces from this campaign alone)
19:52	French "AR24 registered letter" phishing lure sent from the account
19:58 → 00:00	SMTP checker "hit" notices sent to attacker mailboxes (gmail/outlook/hotmail)
21:53 → 1 Apr 01:11	"Emily Portney" bulk-mailer campaign via SMTP AUTH (≈2,500 bounces)
~22:00-22:04	Mail history before this point disappears from INBOX, Sent, Trash, Archives and Archives.2025 (see Unknowns)
22:48	"Leads / databases for sale" spam ("Paul")
23:10 → 1 Apr 00:08	"US Treasury" Bcc blasts via Roundcube (40 × 99 recipients)
1 Apr 01:11	Last submission seen
1 Apr – 10 Apr	Bounces, delayed DSNs, Outlook retry failures (4.7.650) and auto-replies arrive. No new sends.

Volume: about **14,400 bounce notices** (2,145 in "Bounces April 2026", ~12,240 in Trash, plus some in Junk). Microsoft rejected mail from the relay IP 135.181.193.48 citing a **Spamhaus listing**, so this also hurt deliverability on Federated Computer's shared relay.

Still unknown

1. **How the password leaked.** It was long and random, which rules out guessing. That leaves an infostealer (passwords saved in a browser or mail client on a compromised device), a phishing page, or the same password used elsewhere and leaked there.
2. **Source IPs and first login.** NFE's MTA strips submission `Received` headers, so no client IP survives in the bounces. Only server logs can show this: Postfix `sasl_username`, Dovecot auth and Roundcube `userlogins` for 31 Mar 2026. Nextcloud's activity stream only goes back to 27 Apr 2026 and doesn't log logins anyway.
3. **Whether Nextcloud itself was accessed.** The same LDAP password logs into Nextcloud, and **Aaron is in the `admins` group**. No evidence either way survives in the activity stream.
4. **The missing mail history.** INBOX, Sent, Trash, Archives and Archives.2025 contain nothing older than ~22:00 UTC on 31 Mar. Sent's oldest item is spam. Drafts still has Aaron's own drafts back to April 2025. Mail could have been bulk-deleted mid-attack, e.g. to hide bounces. *Open question: did anyone purge these folders or move the mailbox?* If not, ask Federated Computer whether backups from before 31 Mar exist.
5. The app password **"cli" created by an administrator on 13 Oct 2026** should be confirmed as legitimate.

Recommendations (for Aaron to approve. None have been applied.)

Now

- Confirm the rotated password is **not reused anywhere** and that the old one is gone from every saved-password store. The old password appears in clear text in several bounces in Trash and "Bounces April 2026", so treat it as public.
- Delete the "You get a new smtp" / "HIT" / "SMTP Checker" / "Jerry Rivera" bounces that contain the old password.
- Run a malware/infostealer scan on every device that had the password saved (browser and mail client). Check aaron.tushabe@nearlyfreeenergy.com at haveibeenpwned.com.
- Review Nextcloud → Personal settings → Security → Devices & sessions. Revoke anything unrecognised and confirm the "cli" app password.
- Ask Federated Computer for Postfix/Dovecot/Roundcube logs for 31 Mar 2026 18:00–1 Apr 02:00 UTC (logs may already have rotated), and for any pre-31-Mar mailbox backup. Also ask whether 135.181.193.48 is still on Spamhaus lists.

Harden

- **Enable 2FA in Nextcloud** (TOTP), at least for every account in `admins`. Note this alone does **not** protect IMAP/SMTP/Roundcube, which still accept the bare LDAP password.
- **Protect Roundcube**: add a 2FA plugin (e.g. `twofactor_gauthenticator`) or put it behind SSO/VPN. Otherwise retire it in favour of Nextcloud Mail, and keep it on the latest release.
- **Outbound rate limits per authenticated user** on submission: Postfix `smtpd_client_message_rate_limit` / `smtpd_client_recipient_rate_limit`, or `rspamd ratelimit` keyed on `user`. Set Roundcube `max_recipients` (about 20) and `max_group_members`. Add an alert when one user sends more than N messages per hour.
- **fail2ban / rate-limiting on SASL auth failures** for SMTP, IMAP and Roundcube logins.
- **App-password hygiene**: give each client (phone mail app, CLI tools, Claude skills) its own named app password, revoke unused ones, and never save the main password in browsers.
- **DNS** (checked today): SPF is `-all` and covers the relays, but has duplicate entries (`de-relay` and `fi-relay` each listed twice). DKIM selector `mail` is present. DMARC is `p=quarantine; sp=none; pct=100` with reports to admin@. Proposed: tidy the SPF duplicates and move DMARC to `p=reject; sp=reject` after a few weeks of clean aggregate reports. This stops outright spoofing, but would **not** have stopped this incident, since the spam was legitimately signed.
- Check the DMARC aggregate reports at admin@nearlyfreeenergy.com for 31 Mar–1 Apr. They show volume per sending IP.

Second account: dansturn.kimbowa@nearlyfreeenergy.com (May – Sep 2026)

216 bounce notices on Dansturn's account (now in "Bounces 2026", Trash and INBOX) were analysed the same way.

This is also a stolen password used for authenticated sending, not spoofing. All 216 returned originals are DKIM-signed `d=nearlyfreeenergy.com` and have envelope sender `dansturn.kimbowa@...`. They went out through fi-relay, or directly from NFE's server IP 128.140.54.201.

But it looks like a different actor and tool from Aaron's incident:

	Aaron (Mar-Apr)	Dansturn (May-Sep)
Window	One ~6-hour burst (31 Mar 18:52 → 1 Apr 01:11 UTC)	Low-and-slow bursts: 5-6 May, 18 May, 7 Aug, 15-19 Aug, 26 Aug, 29 Aug → 3 Sep 19:25 UTC (last seen)
Route	Roundcube webmail and SMTP AUTH	SMTP AUTH only. Nothing in Sent or Drafts, and Sent history is intact back to Jul 2025
Tooling	SMTP-checker "hit" notices; Roundcube; bulk mailer with <code>YYYYMMDDhhmmss.HEX</code> Message-IDs	Commercial spam mailer: <code>X-Felis-L</code> / <code>X-rpcampaign</code> / <code>List-ID</code> headers, random lowercase Message-IDs, no <code>Date</code> header (added downstream). No checker "hit" messages seen
Content	English advance-fee / loan / "Treasury" scams; reply-to Gmail accounts	German phishing posing as Deutsche Rentenversicherung ("Ihre Daten sind veraltet", May). Dating-spam lures with German personas ("Anna sent a hello...", Aug-Sep), linking to throwaway tracker domains (maileo.app, edgeunite.co.uk and dozens of hacked sites)
Targets	Hotmail/Outlook, Gmail, AU ISPs	web.de / T-Online / freenet (DE), Comcast, Outlook
Bounce volume	~14,400	216 (low because the mailer throttles; real volume unknown)

Conclusion: the entry point is the same *kind*: a valid mailbox password accepted by the LDAP-backed SMTP submission service, which has no 2FA and no per-user rate limit. But nothing links the two incidents to the same actor or the same leak. There is no sign of a server-wide compromise either: team@ and dismas.friday@ show no outbound bounce waves this year. Each password was

most likely leaked separately (infostealer, phishing or reuse) and then sold.

Dansturn-specific actions

- **Urgent: confirm Dansturn's password was changed after 3 Sep 2026.** If not, change it now and treat the account as still compromised. The bounces stopped on 8 Sep, but that may just be the attacker pausing.
- Scan Dansturn's devices for infostealers. Check for reuse of the password elsewhere.
- Include Dansturn's account in the log request to Federated Computer (SASL logins for `dansturn.kimbowa`, May-Sep 2026).
- Side note: T-Online rejects mail sent **directly** from 128.140.54.201 ("Dialup/transient IP not allowed"). Ask Federated Computer why some outbound mail bypasses the relays.

Indicators (attacker-controlled addresses)

Reply-To / hit recipients: `emily.portney37@gmail.com`, `j6919069@gmail.com`,
`samuelbrandon430@gmail.com`, `patriciabloomberg.foundation@gmail.com`, `dannyalba@usa.com`,
`beinspired4730@gmail.com`, `gas.c@outlook.com`, `stephenschwarman252525@hotmail.com`,
`richard.lerbier@gmail.com`, `alugixuge234@gmail.com`.

Lessons for this book

These incidents shaped the [Leaked Credentials Runbook](#), [Accounts, 2FA and App Passwords](#) and the [Audit Logging Policy](#).

Product Security

Securing what NFE builds and deploys in the field: meters, inverters, OpenEMS/Raspberry Pi edge devices, monitoring and code. Adapted from GitLab's Product Security department.

Field Device and Code Security Baseline

Field Device and Code Security Baseline

Adapted from GitLab's Product Security, Vulnerability Management and Secure Coding pages, for NFE's field hardware and software.

What NFE deploys at customer sites (meters, hybrid inverters, OpenEMS on Raspberry Pi, the inverter monitor) controls people's power. A compromise there is an **S1**.

Baseline for every field device (before it leaves for a site)

- ☐ **Default passwords changed** on the inverter, meter, router and Pi (e.g. OpenEMS `admin/admin`, the Pi's default user). Credentials stored in the shared vault.
- ☐ **SSH:** key-based login only; password login and root login disabled.
- ☐ **No direct internet exposure:** no port forwarding to the Pi, OpenEMS UI or Modbus. Remote access only through a VPN or tunnel (Tailscale/WireGuard).
- ☐ **Modbus/TCP and RS-485 stay local.** Modbus has no authentication or encryption; some inverters accept write commands with no password. Restrict writes to the controller that needs them.
- ☐ **Updates:** OS security updates enabled (`unattended-upgrades` on Raspberry Pi OS). Firmware versions recorded.
- ☐ **Notification/alert endpoints** bind to localhost or require a token. See the [inverter-monitor hardening ADR](#).
- ☐ Device recorded in the asset inventory (site, serial, firmware, who has access).

Code we write

- No secrets in code or repositories. Use environment files kept out of version control, or a secret store. Scan repos with `gitLeaks` before pushing (borrowed from GitLab's "gitLeaks on your laptop").
- Review dependencies before adding them, and keep them updated.
- Peer-review changes that touch device control, payments or customer data.

Vulnerabilities

1. Anyone who finds a weakness (in our code, a device, a vendor product) reports it like an incident; see [Reporting a Security Incident](#).
2. The tech lead sets a severity with the [severity matrix](#) and creates a Plane task.
3. Target fix times: **S1 within 24-72 h, S2 within 2 weeks, S3 within 2 months, S4 best effort**. Vendor issues are tracked until the vendor ships a fix, with workarounds (isolation, disabling a feature) in the meantime.

Related pages

- [Running OpenEMS Edge on a Raspberry Pi](#)
- [Metering protocols: DLMS/COSEM, OBIS, Modbus, MQTT](#)