

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](#)
- [Accounts, 2FA and App Passwords](#)
- [Email Security and Phishing](#)
- [Device and Network Security](#)
- [Onboarding and Offboarding Access](#)

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](#).