

# 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](https://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](#).

---

Revision #2

Created 2026-10-20 23:50:01 UTC by MCP Server

Updated 2026-10-21 00:02:09 UTC by MCP Server