

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.

Revision #1

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

Updated 2026-10-21 00:02:14 UTC by MCP Server