

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.