

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](#).

Revision #1

Created 2026-10-20 23:48:55 UTC by MCP Server

Updated 2026-10-21 00:02:08 UTC by MCP Server