

Incident Response

How to report a security incident, how we classify severity, and how we respond. Adapted from GitLab's SIRT pages.

- [Reporting a Security Incident](#)
- [Security Incident Severity Matrix](#)
- [Security Incident Response Guide](#)
- [Leaked Credentials Runbook](#)
- [Responding to Ransomware](#)

Reporting a Security Incident

Reporting a Security Incident

Adapted from GitLab's "Engaging the Security Engineer On-Call".

If in doubt, report it. A false alarm costs a few minutes. An unreported compromise cost us weeks in 2026 (see Incident Reports).

What counts as an incident

- A lost or stolen laptop, phone or USB drive that holds NFE data or saved passwords.
- **Leaked credentials:** your password or an app password typed into a suspicious page, pasted in chat or email, committed to code, or seen by someone else.
- A device that may be infected: pop-ups, unknown apps, antivirus alerts, browser extensions you didn't install.
- **Bounces or replies for mail you never sent.** This is the sign that someone is sending as you.
- Logins, devices or app passwords you don't recognise (Nextcloud → Personal settings → Security).
- Customer, partner or financial data shared with the wrong people.
- Anything strange on field equipment: meters, inverters, Raspberry Pi/OpenEMS devices changing settings on their own, unknown SSH logins.

How to report

1. **Urgent** (you may be compromised right now, or customer power or data is affected):
 - Message the Security DRI directly in Nextcloud Talk **and** phone or WhatsApp them.
 - If you can't reach Talk or your NFE account (e.g. your password was changed), use your personal email or phone. Don't wait.
2. **Not urgent** (a suspicious email you didn't click, a question):
 - Post in the team Talk chat or message the Security DRI. Expect an answer within one working day.

Include:

- what you saw, and when (with timezone);

- which account, device or system;
- what you already did (clicked a link, entered a password, replied);
- screenshots or the original email. **Forward suspicious mail as an attachment; don't just describe it.**

Phishing

- **Didn't engage** (no click, no reply): report it, then delete it or move it to Junk.
- **Engaged** (clicked a link, entered a password, opened an attachment, replied, sent money or gift cards): treat it as **urgent**. Change your password straight away from a device you trust, then report.

What happens next

The Security DRI triages the report, sets a severity using the [severity matrix](#), and follows the [incident response guide](#). You may be asked to stay available to answer questions in the first hour.

Security Incident Severity Matrix

Security Incident Severity Matrix

Adapted from GitLab's Security Incident Severity Matrix.

Purpose

A standard way to classify how serious a security incident is. Severity decides how fast we respond, who gets involved and who we tell. It is set during the first triage.

Matrix

Severity	Impact	NFE response	Examples
S1 Critical	Customers lose power or their data is exposed, or severe damage to NFE (money, reputation, funder trust)	Drop everything. All available team members help. Updates at least every few hours.	Confirmed breach of customer or financial data. An attacker controls an admin account (Nextcloud <code>admins</code> , server root, ERPNext admin). Remote control of meters or inverters at a site. Ransomware on a shared system.
S2 High	Significant disruption for customers or the team, or likely damage to NFE	Named responder; same-day action; daily updates	A mailbox used to send spam (Mar-Apr 2026, Aug-Sep 2026). Suspected unauthorised access to Nextcloud or mail. Malware on a team laptop. Our mail relay IP listed on Spamhaus.
S3 Medium	Moderate impact; work is hampered	Handle within the week alongside normal work	A phishing link clicked but no password entered. Weak config found on a field device with no sign of abuse. Infected device that held no NFE credentials.

Severity	Impact	NFE response	Examples
S4 Low	Minimal impact; workaround available	Normal process / backlog	A policy slip with no sensitive data involved (e.g. a password in a private note, now changed). Phishing reported without engagement.

Things to weigh

- **Confidentiality, integrity, availability:** which of these are affected? The more, the higher the severity.
- **Affected surface:** customer sites and meters → shared servers (Nextcloud, mail, ERPNext, BookStack) → one account → one device.
- **Exploitability:** does it need one command, some effort, or rare conditions?
- **Visibility:** can everyone see it, people with specific access, or only you?
- **Privilege:** members of the Nextcloud `admins` group, server root and field-device admin accounts raise severity by one level.

When unsure, choose the **higher** severity. You can lower it after investigation.

Security Incident Response Guide

Security Incident Response Guide

Adapted from GitLab's Security Incident Response Guide (SIRT).

Scope

Any event that may harm NFE, our customers, partners or team members, or that breaks our security or acceptable-use policies. That includes incidents at providers we depend on, such as Federated Computer (hosting and mail relays). The Security DRI decides whether an event becomes an incident. Reports can come from anyone, inside or outside NFE.

Roles

Role	Responsibility
Team members	Report quickly; follow instructions; preserve evidence (don't delete suspicious mail or files)
Security DRI (incident lead)	Triage, set severity, coordinate the response, keep the incident record, write the report
System owners	Help contain and recover their system (e.g. Federated Computer for mail/LDAP, tech lead for field devices)

Phases

1. **Detection:** a team member, an alert, a partner or a bounce wave tells us something is wrong.
2. **Analysis:** confirm it's real. Set severity with the [matrix](#). Record the start time, systems and accounts involved.

3. **Containment:** stop it spreading.
 - Change the affected passwords.
 - Revoke app passwords and sessions.
 - Disable the account if needed.
 - Isolate the device or take it off the network.
 - Ask the host to pause outbound mail for the account.
4. **Eradication:** remove the attacker's access.
 - Check for forwarding rules, Sieve filters, aliases and new app passwords.
 - Check for unknown SSH keys and installed software.
 - Fix the weakness that let them in.
5. **Recovery:** restore normal operation, add monitoring for a repeat, and confirm with the affected person.
6. **Post-incident:**
 - Hold a short retrospective.
 - Write it up in **Incident Reports** (timeline, root cause, evidence, what's still unknown, actions).
 - Turn the actions into Plane tasks with owners.

Leaked credentials

When a secret has leaked (password, app password, API key, SSH key, token), **revoke it immediately**, even before we know the full impact. A broken integration is cheaper than an abused credential. Then tell the owners of anything that used it. See [Leaked Credentials Runbook](#).

Evidence

- Keep originals. Move suspicious mail and bounces into a folder; don't trash them.
- Note what you did and when (UTC).
- Ask providers for logs early, because logs rotate. For mail, ask Federated Computer for Postfix SASL, Dovecot and Roundcube login logs.
- **Never paste a leaked password into a report, chat or ticket.** Write "old password (redacted)".

Confidentiality

Incident details often include personal or customer data, so share them only with the people who need them. Once the incident is closed, the report is shared in the Library with sensitive details removed. See [Transparency by Default](#).

Leaked Credentials Runbook

Leaked Credentials Runbook

Use this when an NFE password, app password, API key or SSH key may be known to someone else. It was written after the 2026 mailbox compromises.

“ **Important:** at NFE, **one LDAP password** unlocks Nextcloud, IMAP/SMTP mail and Roundcube webmail. A leaked mail password is a leaked Nextcloud password, and for members of `admins`, a leaked admin password.

1. Contain (first hour)

1. **Change the password** from a device you trust. Use a new, random, unique password from a password manager.
2. **Nextcloud → Personal settings → Security → Devices & sessions:**
 - revoke every session and app password you don't recognise;
 - when in doubt, revoke them all and re-create the ones you need.
3. **Mail settings:** check for anything you didn't create.
 - Nextcloud Mail → Account settings → Filters and Autoresponder.
 - Roundcube → Settings → Filters / Identities / Responses.
 - Look for forwarding, redirect or vacation rules and extra identities.
4. Ask the Security DRI to ask **Federated Computer** to:
 - confirm the account is no longer sending;
 - pause outbound mail for it if it still is;
 - share SASL/Roundcube login logs (source IPs, times).

2. Find how it leaked

- **Reuse:** was the same password used anywhere else? Check haveibeenpwned.com for your NFE address.
- **Infostealer:** were passwords saved in a browser or mail app on a device that could be infected? Scan it, and change every password saved on that device.
- **Phishing:** did you type the password into a page reached from an email link?
- **Exposure:** was it pasted in chat, email, a file, a screenshot or code?

3. Clean up

- Delete (with the Security DRI's agreement) any mail or file that contains the old password, e.g. "SMTP checker" bounces.
- Rotate anything that was shared alongside it (shared accounts, API keys in the same note).
- Update every legitimate device with its own **app password**. See [Accounts, 2FA and App Passwords](#).

4. Record

Open an incident record and, when closed, add a report to **Incident Reports**.

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](#).