

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](#).

Revision #1

Created 2026-10-20 23:48:34 UTC by MCP Server

Updated 2026-10-21 00:02:06 UTC by MCP Server