

Vulnerability and Patch Management Policy

Seba Agency UG (haftungsbeschränkt) · Version 1.0 · Effective Oct 13, 2026 · Owner: Joshua Omosebi, Managing Director · Review: annually

1. Purpose and scope

This policy keeps our systems free of known vulnerabilities. It covers the n8n server (Ubuntu, Coolify, Docker, n8n and any community nodes), company laptops and phones, and the SaaS accounts listed in the Access Control Policy.

2. Patch timelines

Component	Routine updates	Critical security fixes
Ubuntu security updates	Installed automatically every day (unattended-upgrades)	Automatic; reboot within 7 days if required
n8n	Within 30 days of a new stable release	Within 72 hours of a published security advisory
Coolify, Docker and other containers	Within 30 days	Within 72 hours
Laptops, phones and browsers	Automatic updates switched on	Within 7 days

A fix counts as critical if the vendor rates it critical or high, or if the vulnerability is known to be actively exploited. If a fix cannot be applied in time, a workaround is applied (switching off the affected feature or restricting access) and recorded in the maintenance log.

3. Monitoring for vulnerabilities

- We follow security advisories for n8n (GitHub security advisories and release notes), Ubuntu (Ubuntu Security Notices) and Coolify (release notes), with notifications switched on [confirm: GitHub “Watch → Releases / Security alerts”].

- We use only official n8n nodes, or community nodes reviewed before installation. Unused nodes, workflows and credentials are removed.

4. Regular checks

Check	Frequency
External port scan of the server: only 80 and 443 open (SSH restricted)	Quarterly
TLS configuration check (e.g. SSL Labs)	Quarterly
Review n8n users, credentials and active workflows; remove what is unused	Quarterly, with the access review
Check 2FA is on for every account in the access register	Quarterly
Confirm backups run, and test a restore	Annually

5. Review

This policy is reviewed annually and after any incident caused by a missing update.