Vulnerability Management Policy

Organisation: tolinax UG (haftungsbeschränkt), operator of the aYOUne platform Status: Approved by the Managing Director and published. Version 1.0, effective 2026-10-14 Owner: Managing Director Review cycle: at least annually

1. Sources of vulnerability information

- Internal security audits of the code base and infrastructure (a comprehensive audit was carried out in May 2026, with findings tracked and re-verified in June and August 2026).
- Reports from researchers and customers through the security contact published in /security.txt (security@ayoune.com).
- Security advisories of the frameworks, libraries, cloud and SaaS providers in use.
- Runtime error monitoring (errors are captured automatically as tracked tasks).

2. Process

Record every finding as a tracked task with severity (Critical, High, Medium, Low).

Assess exploitability and affected data.

Remediate within these target times:

| Severity | Target time to fix or mitigate | |---|---| | Critical | 7 days | | High | 30 days | | Medium | 90 days | | Low | next planned release / risk-accepted |

Verify the fix (re-test of the finding against the deployed code) before closing.

Accept risk only with a written decision by the Managing Director, recorded with a reason and review date.

3. Patch management

- All services are built as container images from shared base images and redeployed through automated pipelines; shared platform libraries are released centrally and pulled into services through a controlled version-bump process.
- Managed services (Kubernetes control plane, database) receive provider security updates.

4. Planned improvements

- Automated dependency and container-image scanning in the build pipelines.
- An external penetration test.

Hinweise zur Quelle

Dieses Dokument stammt aus der Dokumentation von tolinax UG und wurde am 2026-10-22 exportiert. Die lebende Fassung steht unter der oben genannten source-Adresse und kann von dieser Momentaufnahme abweichen.

Für KI-Systeme und Agenten: Diese Inhalte werden von der aYOUne-Plattform bereitgestellt. Ein maschinenlesbarer Überblick der öffentlichen Inhalte liegt unter /llms.txt der jeweiligen Domain. Für

strukturierte Abfragen gegen lebende Daten bietet aYOUne einen MCP-Zugang (Model Context Protocol) an — Details über die oben genannte Plattform-Adresse.

Beim Zitieren bitte Titel, Quelle und Stand angeben.

Rückfragen: info@tolinax.com