# Network Security and Monitoring 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. Architecture (implemented)

- Production runs on Google Kubernetes Engine in europe-west3 (Frankfurt, Germany). The database is a managed MongoDB Atlas cluster in the same region.
- All inbound internet traffic enters through a single service-mesh ingress gateway (Istio). Services are not exposed individually to the internet; only explicitly routed hostnames are reachable.
- Workload classes are separated: crawler workloads run on a dedicated, tainted node pool, isolated from API and worker workloads.
- Real-time media and remote-support relays that need raw TCP/UDP run in their own namespaces behind dedicated load balancers.
- Build and package infrastructure (private package registry, CI runners) is hosted separately at Hetzner in Nuremberg, Germany, and holds no customer data.

## 2. Protective controls (implemented)

- HTTPS-only public endpoints; HTTP is redirected.
- Internal metrics endpoints are blocked at the gateway for external requests.
- IP block lists at the gateway for abusive sources.
- Rate limiting on all APIs (Redis-backed) with stricter limits on login, second-factor, verification and PIN endpoints; account lockout after repeated failures.
- Security headers on API responses (including HSTS).
- Inbound webhooks are accepted only with valid provider signatures.

## 3. Monitoring and detection (implemented)

- Prometheus with Alertmanager collects metrics from the cluster and services; alerts are delivered to the operations team in real time via a messaging channel.
- Dashboards for service health and resource usage.
- Kubernetes health and readiness probes restart unhealthy services automatically.
- Runtime errors of every service are recorded automatically as tracked bug tasks.
- Authentication events and API actions are logged centrally.
- A public status page reports component status and incidents.

## 4. Planned improvements

- Kubernetes network policies (default-deny between namespaces and workloads).
- Strict mutual TLS inside the service mesh with authorisation policies (internal traffic is not yet mutually authenticated).

- Evaluation of a web application firewall in front of the ingress gateway.

## 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