TECHNICAL & ORGANISATIONAL MEASURES (TOM) — VERSION 1.0 · 15.09.2026

Tenant isolation / Mandantentrennung Organisation-scoped entities and server-side authorisation are used; frontend-only filtering is not relied upon for tenant isolation.

Authentication / Authentifizierung Passwords are stored as hashes; setup/reset tokens are stored as hashes. In production, session cookies use HttpOnly, SameSite and Secure.

Agent authentication Agent credentials are stored as hashes; enrollment tokens are hashed, time-limited, revocable and intended for one-time enrollment.

Secret protection / Secrets YCM credentials and PBX API secrets are encrypted at application level. Secrets must not be logged, exposed in HTML or unnecessarily transmitted by email.

Authorization / Berechtigung RBAC and organisation checks are performed server-side. Authorisation state is database-backed; Redis may be used as a non-authoritative cache.

Transport security HTTPS/TLS is required for the public application and Agent communications. Production uses HSTS and baseline security headers.

Browser security X-Content-Type-Options, frame protection, Referrer-Policy, Permissions-Policy and a CSP baseline are configured; unsafe browser requests are controlled.

Rate limiting / Abuse prevention Login throttling and selected API rate limits are implemented; Reflector design uses short-lived authorisation and abuse protection.

Auditability Organisation and platform audit logs record security- and administration-relevant actions with actor, organisation, action, metadata and timestamp where applicable.

Data minimisation Heartbeat persistence updates current state instead of storing one new row per heartbeat; current states are separated from event history.

Resilience / Availability Background jobs are designed for idempotency, locking and retry; PostgreSQL remains the persistent source of truth and Redis is non-authoritative for authorisation.

Deletion A 30-day offboarding and recovery period generally applies after termination. Organisation-scoped data can then be removed through the controlled billing-purge workflow and foreign-key cascades; shared users are preserved where they still belong to another organisation. Evidentiary, audit and billing records required for legal or operational purposes are handled separately. Backups remain protected until the applicable backup lifecycle expires.

Subprocessor governance A current Subprocessor List is maintained; DPA/SCC or other appropriate transfer mechanisms are used where required. Changes to subprocessors that process Customer Data are communicated in accordance with the DPA.

Security incident handling An incident-response procedure covering triage, containment, evidence preservation, customer notification and escalation is documented in the internal Security Incident Runbook.

Access to production data Access to production/customer data is limited to need-to-know/least-privilege. Support access, confidentiality, auditability, revocation and periodic access reviews are governed by the internal Production Support Access Policy.