TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM) — VERSION 1.0 · 15.09.2026

Tenant isolation / Mandantentrennung Organisationsbezogene Entitäten und serverseitige Autorisierung; Frontend-Filterung wird nicht als Mandantentrennung verwendet.

Authentication / Authentifizierung Passwörter werden gehasht gespeichert; Setup-/Reset-Tokens werden als Hashes gespeichert. Session-Cookies verwenden in Produktion HttpOnly, SameSite und Secure.

Agent authentication Agent-Credentials werden als Hashes gespeichert; Enrollment-Tokens sind gehasht, zeitlich begrenzt, widerrufbar und für einmaliges Enrollment vorgesehen.

Secret protection / Secrets YCM-Zugangsdaten und PBX-API-Secrets werden auf Anwendungsebene verschlüsselt. Secrets dürfen nicht geloggt, in HTML offengelegt oder unnötig per E-Mail versendet werden.

Authorization / Berechtigung RBAC- und Organisationsprüfungen erfolgen serverseitig. Berechtigungszustand ist DB-basiert; Redis darf als nicht-autoritärer Cache dienen.

Transport security HTTPS/TLS ist für öffentliche Anwendung und Agent-Kommunikation erforderlich. Produktion verwendet HSTS und grundlegende Security Headers.

Browser security X-Content-Type-Options, Frame-Schutz, Referrer-Policy, Permissions-Policy und CSP-Basis sind konfiguriert; unsichere Browser-Anfragen werden kontrolliert.

Rate limiting / Abuse prevention Login-Throttling und ausgewählte API-Rate-Limits sind implementiert; Reflector-Design verwendet kurzlebige Autorisierung und Missbrauchsschutz.

Auditability Organisations- und Plattform-Audit-Logs protokollieren sicherheits- und administrationsrelevante Aktionen mit Actor, Organisation, Aktion, Metadaten und Zeitstempel, soweit anwendbar.

Data minimisation Heartbeat-Persistenz aktualisiert den aktuellen Zustand statt pro Heartbeat eine neue Zeile zu speichern; aktuelle Zustände werden von Ereignisverläufen getrennt.

Resilience / Verfügbarkeit Background Jobs sind auf Idempotenz, Locking und Retry ausgelegt; PostgreSQL bleibt persistente Source of Truth und Redis ist für Autorisierung nicht autoritativ.

Deletion / Löschung Nach Beendigung gilt grundsätzlich eine 30-tägige Offboarding- und Wiederherstellungsperiode. Organisationsbezogene Daten können anschliessend über den kontrollierten Billing-Purge-Workflow und Foreign-Key-Cascades entfernt werden; gemeinsam genutzte Benutzer bleiben erhalten, wenn sie weiteren Organisationen angehören. Rechtlich oder betrieblich erforderliche Nachweis-, Audit- und Billing-Daten werden getrennt behandelt. Sicherungskopien bleiben bis zum Ablauf des jeweils geltenden Backup-Lebenszyklus geschützt.

Subprocessor governance Eine aktuelle Subprocessor-Liste wird geführt; DPA/SCC bzw. geeignete Transfermechanismen werden nach Bedarf eingesetzt. Änderungen an Unterauftragsbearbeitern, die Kundendaten bearbeiten, werden gemäss DPA kommuniziert.

Security incident handling Ein Incident-Response-Verfahren mit Triage, Eindämmung, Beweissicherung, Kundenbenachrichtigung und Eskalation ist im internen Security Incident Runbook dokumentiert.

Access to production data Zugriff auf Produktions-/Kundendaten erfolgt nur nach Need-to-know/Least-Privilege. Support-Zugriff, Vertraulichkeit, Auditierbarkeit, Widerruf und periodische Zugriffsprüfungen sind in der internen Production Support Access Policy geregelt.