# Vorbereitung SOC 2 Typ II

Trust Service Criteria (AICPA) — Aureus IA SPRL

Aureus Social Pro ist eine belgische SaaS-Lohnverwaltungsplattform. Dieses Dokument bildet die Sicherheitskontrollen auf die AICPA Trust Service Criteria fur die SOC 2 Typ II-Zertifizierung ab.

## 1. Sicherheit (CC6-CC8)

| Kontrolle | Implementierung | Status |
|---|---|---|
| CC6.1 — Logische Zugriffskontrolle | JWT + RBAC + Supabase RLS | OK |
| CC6.2 — Authentifizierung | Email/Passwort + 2FA TOTP | OK |
| CC6.3 — Autorisierungsverwaltung | 5 Rollenebenen | OK |
| CC6.6 — Externe Zugriffsbeschrankungen | Rate Limiting + strenge CORS | OK |
| CC7.1 — Anomalieerkennung | Brute-Force-Erkennung + Warnungen | OK |
| CC7.2 — Vorfallsreaktion | Dokumentiertes Verfahren, 72h-Meldung | OK |
| CC8.1 — Anderungsmanagement | Git PR + Branch Protection | OK |

## 2. Verfugbarkeit (A1)

| Kontrolle | Implementierung | Status |
|---|---|---|
| A1.1 — Kapazitatsverwaltung | Vercel Auto-Scaling, Supabase Pool | OK |
| A1.2 — Geschaftskontinuitat | EU-Failover, 24h-Backup | OK |
| A1.3 — Wiederherstellungstest | Quartalsweise Wiederherstellung | OK |
| A1.4 — Uberwachung | /api/health, 30s-Prufungen | OK |

## 3. Verarbeitungsintegritat (PI1)

| Kontrolle | Implementierung | Status |
|---|---|---|
| PI1.1 — Berechnungsgenauigkeit | 59 automatisierte Lohntests | OK |
| PI1.2 — Eingabevalidierung | INSZ Modulo97, IBAN-Prufung | OK |
| PI1.3 — Fehlererkennung | Error Boundary, Vorab-Lohnvalidierung | OK |
| PI1.4 — Ruckverfolgbarkeit | Audit-Log aller kritischen Aktionen | OK |

## 4. Vertraulichkeit (C1)

| Kontrolle | Implementierung | Status |
|---|---|---|
| C1.1 — Datenklassifizierung | INSZ=Vertraulich, Lohn=Vertraulich | OK |
| C1.2 — Verschlusselung im Transit | TLS 1.3 (HSTS preload) | OK |
| C1.3 — Verschlusselung im Ruhezustand | Supabase AES-256 | OK |
| C1.4 — Maskierung sensibler Daten | INSZ maskiert in UI/Logs | OK |
| C1.5 — Datenzugriffskontrolle | RLS pro tenant_id | OK |

## 5. Datenschutz (P1-P8)

| Kontrolle | Implementierung | Status |
|---|---|---|
| P1.1 — Datenschutzerklarung | Datenschutzrichtlinie in der App | OK |
| P3.1 — Konforme Erhebung | Minimierung, definierter Zweck | OK |
| P5.1 — Individueller Zugang | Mitarbeiterportal | OK |
| P6.1 — Weitergabe an Dritte | DPA unterzeichnet (Supabase, Vercel) | OK |
| P8.1 — Betroffenenrechte | Formular Art.15-22 | OK |

## 6. Zertifizierungsplanung

| Schritt | Zeitrahmen | Budget |
|---|---|---|
| Gap-Analyse mit Prufer | M+1 | 3.000 EUR |
| Remediierung | M+2-4 | 8.000 EUR |
| Bereitschaftsbewertung | M+5 | 3.000 EUR |
| Typ II-Audit (12 Monate) | M+6-18 | 15.000 EUR |
| Gesamt | 19 Monate | 29.000 EUR |