

# SOC 2 Type II Preparation

Trust Service Criteria (AICPA) — Aureus IA SPRL

Aureus Social Pro is a Belgian payroll management SaaS platform. This document maps security controls to AICPA Trust Service Criteria for SOC 2 Type II certification.

## 1. Security (CC6-CC8)

Control	Implementation	Status
CC6.1 — Logical Access Control	JWT + RBAC + Supabase RLS	OK
CC6.2 — Authentication	Email/password + 2FA TOTP	OK
CC6.3 — Authorization Management	5 role levels	OK
CC6.6 — External Access Restrictions	Rate limiting + strict CORS	OK
CC7.1 — Anomaly Detection	Brute force detection + alerts	OK
CC7.2 — Incident Response	Documented procedure, 72h notification	OK
CC8.1 — Change Management	Git PR + branch protection	OK

## 2. Availability (A1)

Control	Implementation	Status
A1.1 — Capacity Management	Vercel auto-scaling, Supabase pool	OK
A1.2 — Business Continuity	EU failover, 24h backup	OK
A1.3 — Recovery Testing	Quarterly restore test	OK
A1.4 — Monitoring	/api/health, 30s checks	OK

## 3. Processing Integrity (PI1)

Control	Implementation	Status
PI1.1 — Calculation Accuracy	59 automated payroll tests	OK
PI1.2 — Input Validation	NISS Modulo97, IBAN check	OK
PI1.3 — Error Detection	Error boundary, pre-payroll validation	OK
PI1.4 — Traceability	Audit log for all critical actions	OK

## 4. Confidentiality (C1)

Control	Implementation	Status
C1.1 — Data Classification	NISS=Confidential, Payroll=Confidential	OK
C1.2 — Encryption in Transit	TLS 1.3 (HSTS preload)	OK
C1.3 — Encryption at Rest	Supabase AES-256	OK
C1.4 — Sensitive Data Masking	NISS masked in UI/logs	OK
C1.5 — Data Access Control	RLS per tenant_id	OK

## 5. Privacy (P1-P8)

Control	Implementation	Status
P1.1 — Privacy Notice	Privacy policy on app	OK
P3.1 — Compliant Collection	Minimization, defined purpose	OK
P5.1 — Individual Access	Employee portal	OK
P6.1 — Third-party Disclosure	Signed DPA (Supabase, Vercel)	OK
P8.1 — Data Subject Rights	Art.15-22 form	OK

## 6. Certification Timeline

Step	Timeline	Budget
Gap analysis with auditor	M+1	EUR 3,000
Remediation	M+2-4	EUR 8,000
Readiness assessment	M+5	EUR 3,000
Type II Audit (12 months)	M+6-18	EUR 15,000
Total	19 months	EUR 29,000