Preparation SOC 2 Type II

Trust Service Criteria (AICPA) — Aureus IA SPRL

Aureus Social Pro est une plateforme SaaS de gestion de paie belge. Ce document presente la cartographie des controles de securite conformes aux Trust Service Criteria de l'AICPA pour la certification SOC 2 Type II.

1. Securite (CC6-CC8)

Controle	Implementation	Status
CC6.1 — Controle d'acces logique	JWT + RBAC + RLS Supabase	OK
CC6.2 — Authentification	Email/password + 2FA TOTP	OK
CC6.3 — Gestion des autorisations	5 niveaux de roles	OK
CC6.6 — Restrictions d'acces externe	Rate limiting + CORS strict	OK
CC7.1 — Detection d'anomalies	Brute force detection + alertes	OK
CC7.2 — Reponse aux incidents	Procedure documentee, notification 72h	OK
CC8.1 — Gestion des changements	Git PR + branch protection	OK

2. Disponibilite (A1)

Controle	Implementation	Status
A1.1 — Gestion de la capacite	Vercel auto-scaling, Supabase pool	OK
A1.2 — Continuite d'activite	Failover EU, backup 24h	OK
A1.3 — Test de restauration	Restore trimestriel	OK
A1.4 — Monitoring	/api/health, checks 30s	OK

3. Integrite du traitement (PI1)

Controle	Implementation	Status
PI1.1 — Exactitude des calculs	59 tests automatises paie	OK
PI1.2 — Validation des entrees	NISS Modulo97, IBAN check	OK
PI1.3 — Detection d'erreurs	Error boundary, validation pre-paie	OK
PI1.4 — Tracabilite	Audit log toutes actions critiques	OK

4. Confidentialite (C1)

Controle	Implementation	Status
C1.1 — Classification des donnees	NISS=Confidentiel, Paie=Confidentiel	OK
C1.2 — Chiffrement en transit	TLS 1.3 (HSTS preload)	OK
C1.3 — Chiffrement au repos	Supabase AES-256	OK
C1.4 — Masquage donnees sensibles	NISS masque dans UI/logs	OK
C1.5 — Controle d'acces donnees	RLS par tenant_id	OK

5. Vie privee (P1-P8)

Controle	Implementation	Status
P1.1 — Notice de confidentialite	Privacy policy sur l'app	OK
P3.1 — Collecte conforme	Minimisation, finalite definie	OK
P5.1 — Acces individuel	Portail employe	OK
P6.1 — Divulgation tiers	DPA signes (Supabase, Vercel)	OK
P8.1 — Droits des personnes	Formulaire Art.15-22	OK

6. Calendrier de certification

Etape	Delai	Budget
Gap analysis avec auditeur	M+1	3.000 EUR
Remediation	M+2-4	8.000 EUR
Readiness assessment	M+5	3.000 EUR
Audit Type II (12 mois)	M+6-18	15.000 EUR
Total	19 mois	29.000 EUR