

# Voorbereiding SOC 2 Type II

Trust Service Criteria (AICPA) — Aureus IA SPRL

Aureus Social Pro is een Belgisch SaaS-loonbeheerplatform. Dit document presenteert de mapping van beveiligingscontroles conform de Trust Service Criteria van AICPA voor SOC 2 Type II-certificering.

## 1. Beveiliging (CC6-CC8)

Controle	Implementatie	Status
CC6.1 — Logische toegangscontrole	JWT + RBAC + RLS Supabase	OK
CC6.2 — Authenticatie	Email/wachtwoord + 2FA TOTP	OK
CC6.3 — Autorisatiebeheer	5 rol niveaus	OK
CC6.6 — Externe toegangsbeperkingen	Rate limiting + strikte CORS	OK
CC7.1 — Anomaliedetectie	Brute force detectie + waarschuwingen	OK
CC7.2 — Incidentrespons	Gedocumenteerde procedure, melding 72u	OK
CC8.1 — Wijzigingsbeheer	Git PR + branch protection	OK

## 2. Beschikbaarheid (A1)

Controle	Implementatie	Status
A1.1 — Capaciteitsbeheer	Vercel auto-scaling, Supabase pool	OK
A1.2 — Bedrijfscontinuïteit	Failover EU, backup 24u	OK
A1.3 — Hersteltest	Kwartaal hersteltest	OK
A1.4 — Monitoring	/api/health, checks 30s	OK

## 3. Verwerkingsintegriteit (PI1)

Controle	Implementatie	Status
PI1.1 — Nauwkeurigheid berekeningen	59 geautomatiseerde loontests	OK
PI1.2 — Invoervalidatie	INSZ Modulo97, IBAN-controle	OK
PI1.3 — Foutdetectie	Error boundary, pre-loon validatie	OK
PI1.4 — Traceerbaarheid	Audit log alle kritieke acties	OK

## 4. Vertrouwelijkheid (C1)

Controle	Implementatie	Status
C1.1 — Gegevensclassificatie	INSZ=Vertrouwelijk, Loon=Vertrouwelijk	OK
C1.2 — Versleuteling in transit	TLS 1.3 (HSTS preload)	OK
C1.3 — Versleuteling in rust	Supabase AES-256	OK
C1.4 — Maskering gevoelige gegevens	INSZ gemaskeerd in UI/logs	OK
C1.5 — Gegevenstoegangscontrole	RLS per tenant_id	OK

## 5. Privacy (P1-P8)

Controle	Implementatie	Status
P1.1 — Privacyverklaring	Privacybeleid op de app	OK
P3.1 — Conforme verzameling	Minimalisatie, doel gedefinieerd	OK
P5.1 — Individuele toegang	Werknemersportaal	OK
P6.1 — Openbaarmaking derden	DPA ondertekend (Supabase, Vercel)	OK
P8.1 — Rechten betrokkenen	Formulier Art.15-22	OK

## 6. Certificeringsplanning

Stap	Termijn	Budget
Gap-analyse met auditor	M+1	3.000 EUR
Remediatie	M+2-4	8.000 EUR
Gereedheidscontrole	M+5	3.000 EUR
Audit Type II (12 maanden)	M+6-18	15.000 EUR
Totaal	19 maanden	29.000 EUR