Voorbereiding ISO 27001:2022

Informatiebeveiligingsmanagementsysteem (ISMS) — Aureus IA SPRL

1. Beveiligingsbeleid

De directie van Aureus IA SPRL verbindt zich ertoe de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te beschermen, te voldoen aan Belgische en Europese wettelijke vereisten (AVG, INSZ-wet), en het ISMS continu te verbeteren via de PDCA-cyclus.

2. Meetbare doelstellingen

Doelstelling	Indicator	Doel
Beschikbaarheid	Maandelijkse uptime	>= 99,9%
Incidenten	Gemiddelde oplostijd	< 4u (kritiek), < 24u (hoog)
Kwetsbaarheden	Kritieke patch-tijd	< 24u
Toegang	Toegangscontrole-audit	100% per kwartaal
Opleiding	Opgeleid personeel	100% per jaar
Backup	Hersteltest	1x/kwartaal geslaagd

3. Risicomatrix

Activum	Dreiging	Impact	Kans	Behandeling
INSZ-database	Datalek	5	1	AES-256, RLS
API v1	DDoS	3	2	Rate limiting 120/min
Admin-accounts	Compromittering	5	2	2FA + waarschuwing
Broncode	Diefstal	4	1	Branch protection + review
Backup	Gegevensverlies	5	1	Multi-regio + JSON-export
Infrastructuur	Onbeschikbaarheid	4	1	Failover EU secundair
Sessies	Hijacking	4	2	CSP strict + HttpOnly
Loonfiches	Rekenfout	3	2	59 geautomatiseerde tests
Personeel	Menselijke fout	3	3	Onboarding + procedures
Onderaannemers	Niet-conform	4	1	DPA + audit

4. Verklaring van Toepasselijkheid (Bijlage A)

Controle	Beschrijving	Status
A.5.1	Informatiebeveiligingsbeleid	OK
A.5.2	Rollen en verantwoordelijkheden	OK
A.5.3	Functiescheiding	OK
A.8.1	Identificatie van activa	OK
A.8.5	Beveiligde authenticatie	OK
A.8.7	Bescherming tegen malware	OK
A.8.8	Kwetsbaarheidsbeheer	OK
A.8.12	Preventie van datalekken	OK
A.8.15	Logging	OK
A.8.16	Monitoring en bewaking	OK
A.8.24	Gebruik van cryptografie	OK
A.8.25	Veilige ontwikkelingscyclus	OK
A.8.29	Beveiligingstests	OK
A.8.31	Scheiding van omgevingen	OK
A.8.32	Wijzigingsbeheer	OK

5. Bedrijfscontinuiteitsplan (BCP/DRP)

RPO: 24u — RTO: 4u

Scenario	Impact	Actie	Termijn
Vercel-storing	App onbereikbaar	DNS-failover naar backup	1u
Supabase primair storing	Data onbeschikbaar	Overschakeling EU-Central	2u
Database-corruptie	Data beschadigd	Herstel JSON-backup	4u
Account-compromittering	Ongeoorloofde toegang	Tokens intrekken + audit	1u
DDoS-cyberaanval	Verminderde service	WAF Vercel + rate limit	30min

6. Certificeringsplanning

Stap	Termijn	Budget
Interne audit (gap-analyse)	M+1	2.000 EUR
Remediatie van afwijkingen	M+2-3	5.000 EUR
Audit Fase 1	M+4	4.000 EUR
Audit Fase 2	M+5	6.000 EUR
Totaal	5 maanden	17.000 EUR