

Vorbereitung ISO 27001:2022

Informationssicherheitsmanagementsystem (ISMS) — Aureus IA SPRL

1. Informationssicherheitspolitik

Die Geschäftsführung von Aureus IA SPRL verpflichtet sich, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen, die belgischen und europäischen gesetzlichen Anforderungen (DSGVO, INSZ-Gesetz) einzuhalten und das ISMS über den PDCA-Zyklus kontinuierlich zu verbessern.

2. Messbare Ziele

Ziel	Indikator	Zielwert
Verfügbarkeit	Monatliche Uptime	>= 99,9%
Vorfälle	Mittlere Lösungszeit	< 4h (kritisch), < 24h (hoch)
Schwachstellen	Kritische Patch-Zeit	< 24h
Zugang	Zugangsüberprüfungsrate	100% vierteljährlich
Schulung	Geschultes Personal	100% jährlich
Backup	Wiederherstellungstest	1x/Quartal bestanden

3. Risikomatrix

Aktivum	Bedrohung	Auswirkung	Wahrsch.	Behandlung
INSZ-Datenbank	Datenleck	5	1	AES-256, RLS
API v1	DDoS	3	2	Rate Limiting 120/min
Admin-Konten	Kompromittierung	5	2	2FA + Warnung
Quellcode	Diebstahl	4	1	Branch Protection + Review
Backup	Datenverlust	5	1	Multi-Region + JSON-Export
Infrastruktur	Nichtverfügbarkeit	4	1	EU-Failover sekundär
Sitzungen	Hijacking	4	2	CSP strict + HttpOnly
Gehaltszettel	Rechenfehler	3	2	59 automatisierte Tests
Personal	Menschlicher Fehler	3	3	Onboarding + Verfahren
Unterauftragnehmer	Nicht-Konformität	4	1	DPA + Audit

4. Erklärung zur Anwendbarkeit (Anhang A)

Kontrolle	Beschreibung	Status
A.5.1	Informationssicherheitspolitik	OK
A.5.2	Rollen und Verantwortlichkeiten	OK
A.5.3	Aufgabentrennung	OK
A.8.1	Identifikation von Vermögenswerten	OK
A.8.5	Sichere Authentifizierung	OK
A.8.7	Malware-Schutz	OK
A.8.8	Schwachstellenmanagement	OK
A.8.12	Datenleckprävention	OK
A.8.15	Protokollierung	OK
A.8.16	Überwachung	OK
A.8.24	Einsatz von Kryptographie	OK
A.8.25	Sicherer Entwicklungszyklus	OK
A.8.29	Sicherheitstests	OK
A.8.31	Trennung von Umgebungen	OK
A.8.32	Anderungsmanagement	OK

5. Geschäftskontinuitätsplan (BKP/DRP)

RPO: 24h — RTO: 4h

Szenario	Auswirkung	Massnahme	Zeitraumen
Vercel-Ausfall	App nicht erreichbar	DNS-Failover zum Backup	1h
Supabase-Ausfall primar	Daten nicht verfügbar	Umschaltung EU-Central	2h
DB-Korruption	Daten beschädigt	JSON-Backup wiederherstellen	4h
Konto-Kompromittierung	Unbefugter Zugriff	Token widerrufen + Audit	1h
DDoS-Angriff	Eingeschränkter Service	WAF Vercel + Rate Limit	30min

6. Zertifizierungsplanung

Schritt	Zeitraumen	Budget
Internes Audit (Gap-Analyse)	M+1	2.000 EUR
Behebung der Abweichungen	M+2-3	5.000 EUR
Audit Stufe 1	M+4	4.000 EUR
Audit Stufe 2	M+5	6.000 EUR
Gesamt	5 Monate	17.000 EUR