ISO 27001:2022 Preparation

Information Security Management System (ISMS) — Aureus IA SPRL

1. Information Security Policy

The Management of Aureus IA SPRL commits to protecting the confidentiality, integrity and availability of information, complying with Belgian and European legal requirements (GDPR, NISS law), and continuously improving the ISMS through the PDCA cycle.

2. Measurable Objectives

Objective	Indicator	Target
Availability	Monthly uptime	>= 99.9%
Incidents	Mean resolution time	< 4h (critical), < 24h (high)
Vulnerabilities	Critical patch time	< 24h
Access	Access review rate	100% quarterly
Training	Security trained staff	100% annually
Backup	Restore test	1x/quarter passed

3. Risk Matrix

Asset	Threat	Impact	Likeli.	Treatment
NISS Database	Data breach	5	1	AES-256 encryption, RLS
API v1	DDoS / overload	3	2	Rate limiting 120/min
Admin accounts	Credential compromise	5	2	Mandatory 2FA + alerts
Source code	Theft / sabotage	4	1	Branch protection + review
Backup	Data loss	5	1	Multi-region + JSON export
Infrastructure	Unavailability	4	1	EU secondary failover
Sessions	Hijacking	4	2	Strict CSP + HttpOnly
Payslips	Calculation error	3	2	59 automated tests
Staff	Human error	3	3	Onboarding + procedures
Subcontractors	Non-compliance	4	1	Signed DPA + audit

4. Statement of Applicability (Annex A)

Control	Description	Status
A.5.1	Information security policies	OK
A.5.2	Roles and responsibilities	OK
A.5.3	Segregation of duties	OK
A.8.1	Asset identification	OK
A.8.5	Secure authentication	OK
A.8.7	Malware protection	OK
A.8.8	Vulnerability management	OK
A.8.12	Data leakage prevention	OK
A.8.15	Logging	OK
A.8.16	Monitoring	OK
A.8.24	Use of cryptography	OK
A.8.25	Secure development lifecycle	OK
A.8.29	Security testing	OK
A.8.31	Environment separation	OK
A.8.32	Change management	OK

5. Business Continuity Plan (BCP/DRP)

RPO: 24h — RTO: 4h

Scenario	Impact	Action	Timeline
Vercel outage	App inaccessible	DNS failover to backup	1h
Primary Supabase outage	Data unavailable	Switch to EU-Central	2h
DB corruption	Data altered	Restore JSON backup	4h
Account compromise	Unauthorized access	Revoke tokens + audit	1h
DDoS attack	Degraded service	Vercel WAF + rate limit	30min

6. Certification Timeline

Step	Timeline	Budget
Internal audit (gap analysis)	M+1	EUR 2,000
Gap remediation	M+2-3	EUR 5,000
Stage 1 Audit	M+4	EUR 4,000
Stage 2 Audit	M+5	EUR 6,000
Total	5 months	EUR 17,000