Preparation ISO 27001:2022

Systeme de Management de la Securite de l'Information — Aureus IA SPRL

1. Politique de securite

La Direction de Aureus IA SPRL s'engage a proteger la confidentialite, l'integrite et la disponibilite des informations, a se conformer aux exigences legales belges et europeennes (RGPD, loi NISS), et a ameliorer continuellement le SMSI via le cycle PDCA.

2. Objectifs mesurables

Objectif	Indicateur	Cible
Disponibilite	Uptime mensuel	>= 99,9%
Incidents	Temps moyen de resolution	< 4h (critique), < 24h (haute)
Vulnerabilites	Temps de patch critique	< 24h
Acces	Taux de revue des acces	100% trimestriel
Formation	Personnel forme securite	100% annuel
Backup	Test de restauration	1x/trimestre reussi

3. Matrice des risques

Actif	Menace	Impact	Prob.	Traitement
Base de donnees NISS	Fuite de donnees	5	1	Chiffrement AES-256, RLS
API v1	DDoS / surcharge	3	2	Rate limiting 120/min
Comptes admin	Compromission	5	2	2FA obligatoire + alerte
Code source	Vol / sabotage	4	1	Branch protection + review
Backup	Perte de donnees	5	1	Multi-region + export JSON
Infrastructure	Indisponibilite	4	1	Failover EU secondary
Sessions	Hijacking	4	2	CSP strict + HttpOnly
Fiches de paie	Erreur calcul	3	2	59 tests automatises
Personnel	Erreur humaine	3	3	Onboarding + procedures
Sous-traitants	Non-conformite	4	1	DPA signes + audit

4. Declaration d'Applicabilite (Annexe A)

Controle	Description	Status
A.5.1	Politiques de securite de l'information	OK
A.5.2	Roles et responsabilites	OK
A.5.3	Separation des taches	OK
A.8.1	Identification des actifs	OK
A.8.5	Authentification securisee	OK
A.8.7	Protection contre malware	OK
A.8.8	Gestion des vulnerabilites	OK
A.8.12	Prevention fuite de donnees	OK
A.8.15	Journalisation	OK
A.8.16	Surveillance et monitoring	OK
A.8.24	Utilisation de la cryptographie	OK
A.8.25	Cycle de developpement securise	OK
A.8.29	Tests de securite	OK
A.8.31	Separation des environnements	OK
A.8.32	Gestion des changements	OK

5. Plan de continuite (PCA/PRA)

RPO (Recovery Point Objective) : 24h — RTO (Recovery Time Objective) : 4h

Scenario	Impact	Action	Delai
Panne Vercel	App inaccessible	Failover DNS vers backup	1h
Panne Supabase primaire	Donnees indisponibles	Bascule EU-Central	2h
Corruption BDD	Donnees alterees	Restore backup JSON	4h
Compromission compte	Acces non autorise	Revoke tokens + audit	1h
Cyberattaque DDoS	Service degrade	WAF Vercel + rate limit	30min

6. Calendrier de certification

Etape	Delai	Budget
Audit interne (gap analysis)	M+1	2.000 EUR
Remediation des ecarts	M+2-3	5.000 EUR
Audit Stage 1	M+4	4.000 EUR
Audit Stage 2	M+5	6.000 EUR
Total	5 mois	17.000 EUR