Déclaration d'Applicabilité (SoA) — ISO 27001:2022

Statement of Applicability | Organisation : _____ | Date : ___/___/_____ | Version : ___

Instructions : Pour chaque contrôle, indiquez : **Applicable** (O/N), **Justification** d'inclusion ou d'exclusion, **Implémenté** (O/N/Partiel), et le **Document/preuve** associé. La SoA est un livrable obligatoire pour la certification ISO 27001.

A.5 — Contrôles organisationnels

Réf.	Contrôle	Appl.	Justification inclusion/exclusion	Impl.	Document/Preuve
A.5.1	Politiques de sécurité de l'information				
A.5.2	Rôles et responsabilités				
A.5.3	Séparation des tâches				
A.5.4	Responsabilités de la direction				
A.5.5	Contact avec les autorités				
A.5.6	Contact avec groupes d'intérêt				
A.5.7	Renseignement sur les menaces				
A.5.8	Sécurité gestion de projet				
A.5.9	Inventaire informations et actifs				
A.5.10	Utilisation acceptable				
A.5.11	Restitution des actifs				
A.5.12	Classification de l'information				
A.5.13	Étiquetage de l'information				
A.5.14	Transfert de l'information				
A.5.15	Contrôle d'accès				
A.5.16	Gestion des identités				
A.5.17	Informations d'authentification				
A.5.18	Droits d'accès				
A.5.19	Sécurité relations fournisseurs				
A.5.20	Sécurité accords fournisseurs				
A.5.21	Gestion sécurité chaîne TIC				
A.5.22	Surveillance services fournisseurs				
A.5.23	Sécurité services cloud				
A.5.24	Planification gestion incidents				
A.5.25	Évaluation événements sécurité				
A.5.26	Réponse aux incidents				
A.5.27	Enseignements des incidents				
A.5.28	Collecte de preuves				
A.5.29	Sécurité pendant perturbation				
A.5.30	Préparation TIC continuité				
A.5.31	Exigences légales/contractuelles				
A.5.32	Propriété intellectuelle				

A.5.33	Protection enregistrements				
A.5.34	Vie privée et DCP				
A.5.35	Revue indépendante				
A.5.36	Conformité politiques/normes				
A.5.37	Procédures documentées				

A.6 — Contrôles personnes | A.7 — Contrôles physiques

Réf.	Contrôle	Appl.	Justification	Impl.	Document/Preuve
A.6.1	Sélection des candidats				
A.6.2	Conditions d'emploi				
A.6.3	Sensibilisation et formation				
A.6.4	Processus disciplinaire				
A.6.5	Responsabilités fin de contrat				
A.6.6	Accords de confidentialité				
A.6.7	Travail à distance				
A.6.8	Signalement événements sécurité				
A.7.1	Périmètres sécurité physique				
A.7.2	Entrées physiques				
A.7.3	Sécurité bureaux et locaux				
A.7.4	Surveillance sécurité physique				
A.7.5	Menaces environnementales				
A.7.6	Travail zones sécurisées				
A.7.7	Bureau propre / écran verrouillé				
A.7.8	Emplacement matériel				
A.7.9	Actifs hors locaux				
A.7.10	Supports de stockage				
A.7.11	Services généraux				
A.7.12	Sécurité du câblage				
A.7.13	Maintenance matériel				
A.7.14	Mise au rebut sécurisée				

A.8 — Contrôles technologiques

Réf.	Contrôle	Appl.	Justification	Impl.	Document/Preuve
A.8.1	Terminaux utilisateurs				
A.8.2	Droits d'accès privilégiés				
A.8.3	Restriction accès information				
A.8.4	Accès code source				
A.8.5	Authentification sécurisée				
A.8.6	Gestion des capacités				

A.8.7	Protection malwares				
A.8.8	Gestion vulnérabilités techniques				
A.8.9	Gestion de la configuration				
A.8.10	Suppression de l'information				
A.8.11	Masquage des données				
A.8.12	Prévention fuite données				
A.8.13	Sauvegarde information				
A.8.14	Redondance installations				
A.8.15	Journalisation				
A.8.16	Activités de surveillance				
A.8.17	Synchronisation horloges				
A.8.18	Programmes utilitaires privilégiés				
A.8.19	Installation logiciels				
A.8.20	Sécurité réseaux				
A.8.21	Sécurité services réseau				
A.8.22	Séparation réseaux				
A.8.23	Filtrage web				
A.8.24	Cryptographie				
A.8.25	Développement sécurisé				
A.8.26	Exigences sécurité applicatives				
A.8.27	Architecture ingénierie sécurisée				
A.8.28	Codage sécurisé				
A.8.29	Tests sécurité développement				
A.8.30	Développement externalisé				
A.8.31	Séparation environnements				
A.8.32	Gestion changements				
A.8.33	Informations de test				
A.8.34	Protection systèmes d'audit				