					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P23S					Titre du document : **Politique de synchronisation de l'heure**							
Version : 1.0		Date d'entrée en vigueur : 01.01.2025			Propriétaire du document :							
X	Politique		Norme		Procédure		Formulaire		Registre		Autre	

Historique des révisions				
Numéro de révision	**Date de révision**	**Modifications**	**Revu par**	**Propriétaire du processus**

Approbations			
Nom	**Fonction**	**Date**	**Signature**

Alignement sur les normes et réglementations

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	Clause 8	Exigences de contrôle pertinentes
ISO/IEC 27002:2022	Mesure 8	Fonctionnement synchronisé des systèmes
NIST SP 800-53 Rév. 5	SC-45, AU-8	NTP de confiance et exactitude des horodatages des journaux
RGPD de l'UE	Articles 5(1)(d), 32	Exactitude, responsabilité et intégrité des données à caractère personnel au moyen d'horodatages synchronisés
NIS2 de l'UE	Article 21(2)(d)	Capacités de surveillance et de détection soutenues par des journaux synchronisés
DORA de l'UE	Articles 10, 15	Résilience opérationnelle et exactitude des enregistrements techniques
COBIT 2019	DSS05.02, MEA03	Horodatage des événements et surveillance fondée sur des éléments probants

1. Objet

1.1 La présente politique définit les contrôles obligatoires visant à maintenir une heure exacte et synchronisée sur l'ensemble des systèmes qui stockent, transmettent ou traitent les données de l'organisation.

1.2 La synchronisation de l'heure est essentielle pour garantir la traçabilité des journaux système, la corrélation exacte des incidents de sécurité et l'exploitabilité des éléments de preuve dans le cadre d'analyses forensiques ou de revues juridiques.

1.3 L'organisation impose la synchronisation automatisée de l'heure comme exigence fondamentale pour l'intégrité des audits, la réponse aux incidents et la conformité réglementaire au titre de l'ISO 27001, du RGPD, de DORA et de NIS2.

1.4 La présente politique garantit que tous les systèmes utilisent des sources de temps de confiance, interdit le contournement manuel des paramètres d'heure et impose la correction rapide des dérives d'horloge.

2. Champ d'application

2.1 La présente politique s'applique à :

2.1.1 Tous les systèmes et équipements appartenant à l'entreprise, y compris les serveurs, postes de travail fixes, ordinateurs portables, appareils mobiles, pare-feu, routeurs et machines virtuelles

2.1.2 L'infrastructure distante et les systèmes hébergés dans le cloud utilisés dans le cadre des opérations (par exemple AWS, Microsoft 365, plateformes SaaS)

2.1.3 Les systèmes qui génèrent ou stockent des journaux d'événements, des enregistrements d'authentification ou des pistes d'audit

2.1.4 Tout employé, prestataire, fournisseur ou prestataire de support informatique chargé de configurer ou de maintenir ces systèmes

2.2 La politique s’applique également aux terminaux BYOD utilisés pour accéder aux systèmes métier, dès lors que ces terminaux stockent ou génèrent des données pertinentes pour l’audit.

3. Objectifs

3.1 Garantir que tous les systèmes critiques synchronisent automatiquement l’heure au moyen de serveurs Network Time Protocol (NTP) de confiance ou de mécanismes équivalents fournis par les prestataires cloud

3.2 Empêcher les écarts horaires susceptibles de compromettre la fiabilité ou la corrélation des journaux système lors des audits ou des investigations de sécurité

3.3 Permettre la détection et la correction en temps utile des dérives horaires au-delà des seuils acceptables

3.4 Maintenir un horodatage cohérent entre les environnements sur site, cloud et distants

3.5 Répondre aux exigences techniques et juridiques d’intégrité, de traçabilité et de non-répudiation des enregistrements et des événements

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Approuve la présente politique et veille à la conformité de l’organisation

4.1.2 Supervise les revues périodiques de l’exactitude de l’heure au niveau des systèmes et des écarts de mise en œuvre

4.1.3 Approuve les dérogations à la synchronisation automatisée de l’heure, lorsqu’elles sont justifiées et documentées

4.2 Prestataire de support informatique / fonction informatique interne

4.2.1 Configure la synchronisation de l’heure pour tous les systèmes appartenant à l’entreprise ou administrés par celle-ci

4.2.2 Vérifie quotidiennement, ou selon une fréquence planifiée, le bon fonctionnement de la synchronisation

4.2.3 Analyse et corrige les événements de dérive horaire, les échecs de synchronisation ou les problèmes d’accès au NTP

4.2.4 Documente l’état de la synchronisation de l’heure dans le cadre des contrôles mensuels de bon fonctionnement des systèmes

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Exigences de revue et de mise à jour

9.1 Revue planifiée

9.1.1 La présente politique doit faire l’objet d’une revue annuelle par le directeur général, le prestataire de support informatique et le coordinateur à la protection des données

9.1.2 Tous les journaux et rapports d’état de conformité relatifs à la synchronisation de l’heure doivent être pris en compte lors de cette revue

9.2 Mises à jour déclenchées par événement

9.2.1 La présente politique doit être mise à jour si :

9.2.1.1 Une défaillance système entraîne une dérive horaire significative

9.2.1.2 Un audit révèle des défaillances dans la synchronisation de l’heure

9.2.1.3 L’organisation adopte de nouveaux environnements cloud, hybrides ou virtualisés

9.2.1.4 Des évolutions juridiques ou réglementaires introduisent de nouvelles exigences relatives à l’intégrité de l’heure

9.3 Gestion des versions et communication

9.3.1 Toutes les mises à jour doivent être versionnées et datées

9.3.2 Les changements majeurs doivent être communiqués à l'ensemble du personnel technique

9.3.3 Les versions précédentes doivent être conservées pendant 3 ans à des fins d'audit

10. Politiques associées et articulations

10.1 La présente politique doit être appliquée conjointement avec les politiques PME suivantes :

10.1.1 P22S – Politique de journalisation et de surveillance : garantit un horodatage cohérent entre les journaux à des fins de traçabilité et de corrélation forensique.

10.1.2 P30S – Politique de réponse aux incidents : repose sur l'exactitude des horodatages pour reconstituer les incidents, établir les chronologies et étayer les décisions de notification.

10.1.3 P17S – Politique de protection des données et de la vie privée : garantit que les journaux d'accès et les chronologies de traitement des données impliquant des données à caractère personnel sont exacts et défendables au regard du RGPD.

10.1.4 P12S – Politique de gestion des actifs : soutient l'identification des systèmes nécessitant une synchronisation, en particulier les appareils mobiles et distants.

10.1.5 P26S – Politique de sécurité des tiers et des fournisseurs : garantit contractuellement que les fournisseurs qui accèdent aux données de l'organisation ou les journalisent appliquent des pratiques de synchronisation de l'heure.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001 :

11.1.1 Clause 8.1 – Exige la mise en œuvre des contrôles nécessaires à des opérations sécurisées, y compris la journalisation et l'horodatage.

11.2 ISO/IEC 27002 :

11.2.1 Mesure 8.17 – Recommande une heure synchronisée pour tous les systèmes qui produisent des journaux ou fonctionnent de manière coordonnée.

11.3 NIST SP 800-53 Rév. 5 :

11.3.1 AU-8 – Exige l'utilisation de sources de temps internes ou externes pour garantir l'exactitude des horodatages des journaux.

11.3.2 SC-45 – Précise l'utilisation de sources NTP de confiance et l'interdiction des changements manuels d'heure dans les systèmes critiques.

11.4 RGPD de l'UE :

11.4.1 Article 5(1)(d) – Exige l'exactitude et la responsabilité dans le traitement des données à caractère personnel, soutenues par des horodatages synchronisés.

11.4.2 Article 32 – Exige des mesures de sécurité garantissant l'intégrité des données, y compris des plages de journalisation cohérentes.

11.5 Directive NIS2 de l'UE :

11.5.1 Article 21(2)(d) – Exige des capacités de surveillance et de détection, soutenues par des journaux système synchronisés.

11.6 DORA de l'UE :

11.6.1 Article 10 – Exige une résilience opérationnelle, nécessitant des journaux d'incidents TIC traçables et horodatés.

11.6.2 Article 15 – Exige des prestataires de services qu'ils tiennent des enregistrements techniques exacts, y compris une piste d'audit horodatée.

11.7 COBIT 2019 :

11.7.1 DSS05.02 – Souligne l’intégrité des horodatages pour détecter les événements et y répondre.

11.7.2 MEA03.01 – Exige une surveillance des performances fondée sur des éléments probants, étayée par des données exactes et synchronisées dans le temps.