					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P23					Titre du document : **Politique de synchronisation temporelle**							
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	-
ISO/IEC 27002:2022	Mesure 8	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
RGPD de l'UE	Article 32	-
NIS2 de l'UE	Article 21(2)(e)	-
DORA de l'UE	Articles 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Objet

1.1 La présente politique vise à garantir que l'ensemble des systèmes d'information, applications, équipements et services cloud de l'organisation maintiennent des paramètres temporels cohérents et exacts au moyen d'une synchronisation avec des sources de temps désignées et fiables.

1.2 Une synchronisation temporelle exacte est essentielle à la fiabilité de la journalisation, à la sécurité des communications, à la traçabilité d'audit, à la réponse aux incidents et à l'analyse forensique. Un décalage temporel peut entraîner des journaux non corrélables, des échecs d'authentification et des déclarations réglementaires incomplètes.

1.3 La présente politique soutient la mesure 8.17 de l'annexe A de l'ISO/IEC 27001 ainsi que les normes internationales associées, en imposant l'exactitude temporelle et la détection de la dérive d'horloge sur l'ensemble du parc informatique de l'organisation.

2. Champ d’application

2.1 La présente politique s'applique à :

2.1.1 Tous les composants d'infrastructure, y compris les serveurs, postes de travail, équipements réseau, pare-feu et systèmes de l'Internet des objets (IoT)

2.1.2 Tous les environnements virtualisés et cloud (par exemple AWS, Azure, Google Cloud)

2.1.3 Tous les systèmes participant à la journalisation, à l'authentification, au traitement des transactions ou à la corrélation des événements de sécurité

2.1.4 Tous les employés, prestataires et fournisseurs de services tiers responsables de systèmes sensibles au temps

2.2 Les systèmes qui génèrent ou consomment des enregistrements horodatés — tels que des entrées de journal, des alertes, des enregistrements d'activité utilisateur ou des éléments de preuve forensiques — sont réputés relever du champ d'application.

3. Objectifs

3.1 Définir une architecture cohérente et centralisée de synchronisation temporelle au moyen de sources NTP approuvées ou de mécanismes équivalents.

3.2 Garantir que tous les systèmes synchronisent leurs horloges à des intervalles définis et que toute dérive soit détectée et corrigée automatiquement ou avec une intervention minimale.

3.3 Maintenir l'exactitude des horloges dans les environnements hybrides, sur site et cloud afin de permettre :

3.3.1 Une corrélation fiable des événements et une réponse aux incidents efficace

3.3.2 La conformité aux normes et réglementations telles que l'ISO 27001, le RGPD, NIS2 et DORA

3.3.3 Une protection contre les attaques par rejeu et les échecs d'authentification fondés sur le temps

3.4 Établir des rôles clairs, des procédures de gestion des exceptions et des mécanismes d'audit afin d'assurer l'application de la politique.

3.5 Garantir que les anomalies temporelles fassent l'objet d'une journalisation, d'une alerte et d'une escalade lorsqu'elles dépassent les seuils de tolérance.

4. Rôles et responsabilités

4.1 Responsable de la sécurité des systèmes d'information (RSSI)

4.1.1 Est responsable de la présente politique et veille à son alignement avec les contrôles opérationnels du système de management de la sécurité de l'information (SMSI) et les exigences réglementaires.

4.1.2 Approuve le choix des sources de temps de l'entreprise et valide les processus de reporting relatifs à la synchronisation temporelle.

4.2 Responsable des services d'infrastructure / Responsable de l'ingénierie réseau

4.2.1 Assure le maintien en conditions opérationnelles des serveurs NTP primaires et secondaires de l'organisation ou de la configuration des sources temporelles désignées.

4.2.2 Veille à ce que tous les équipements connectés au réseau et toutes les instances virtuelles synchronisent l'heure à des intervalles appropriés.

4.2.3 Assure la surveillance des journaux de synchronisation temporelle, des alertes de dérive d'horloge et des conditions de défaillance.

[... 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 La présente politique doit faire l'objet d'une revue annuelle, ou plus tôt dans les cas suivants :

9.1.1 Détection de codes d'exploitation fondés sur le temps ou de défaillances de journalisation

9.1.2 Modifications de l'infrastructure temporelle principale (par exemple nouveaux serveurs NTP d'entreprise ou mises à jour de protocole)

9.1.3 Écarts de dérive temporelle sur des plateformes cloud ou changements de services régionaux

9.1.4 Résultats post-incident identifiant un décalage temporel comme facteur contributif

9.2 La revue doit être coordonnée par le responsable Infrastructure, avec la contribution requise du SOC, de la sécurité applicative et des parties prenantes de la conformité.

9.3 Les révisions doivent être documentées dans le registre documentaire du SMSI et communiquées aux parties prenantes internes et tierces concernées.

9.4 Les versions historiques de la politique doivent être archivées de manière sécurisée, faire l'objet d'une gestion de versions et être mises à disposition pour les demandes d'audit de conformité ou d'audit juridique.

10. Politiques associées et articulations

10.1 P1 – Politique de sécurité de l'information. Établit le cadre général visant à garantir l'intégrité et la traçabilité de tous les systèmes d'information, dont l'exactitude temporelle constitue un fondement essentiel.

10.2 P5 – Politique de gestion des changements. Encadre les modifications des configurations système, y compris les ajustements des sources temporelles, en imposant une documentation, des tests et des plans de retour arrière appropriés.

10.3 P22 – Politique de journalisation et de surveillance. Dépend directement d'une heure synchronisée afin de garantir l'ordonnancement des événements, la corrélation des journaux et l'intégrité des investigations sur incident entre des systèmes hétérogènes.

10.4 P30 – Politique de réponse aux incidents. Repose sur des horodatages exacts pour les analyses forensiques, les chronologies d'incident et les éléments de preuve relevant de la chaîne de conservation. Une heure inexacte porte atteinte à la crédibilité des rapports d'incident.

10.5 P20 – Politique de protection des terminaux / logiciels malveillants. Exige une génération d'alertes et une analyse comportementale fondées sur une heure exacte afin de détecter la propagation de logiciels malveillants, les mouvements latéraux et les anomalies d'accès.

10.6 P6 – Politique de gestion des risques. Définit le traitement de la désynchronisation comme un risque opérationnel et forensique potentiel, nécessitant les contrôles définis dans la présente politique pour en atténuer l'impact.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Planification et maîtrise opérationnelles : exige l'intégration de contrôles techniques précis, tels que des horloges système synchronisées, pour une exécution opérationnelle fiable.

11.2 ISO/IEC 27002:2022 – Mesure 8

11.2.1 Renforce l'exactitude des horloges et impose la cohérence organisationnelle de l'heure système afin de faciliter la comparaison des journaux, l'investigation et la validation sécurisée des transactions.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – Synchronisation temporelle du système : exige une synchronisation temporelle au moyen de sources faisant autorité sur l'ensemble des composants à l'intérieur du périmètre du système.

11.3.2 AU-8 – Horodatages : garantit l'horodatage exact des événements et fournit la traçabilité nécessaire à l'audit et à la réponse aux incidents.

11.4 RGPD de l'UE (2016/679)

11.4.1 Article 32 – Sécurité du traitement : sans viser explicitement la synchronisation temporelle, impose l'utilisation de mesures techniques appropriées — y compris des pistes d'audit et des journaux — dont la validité et l'intégrité reposent intrinsèquement sur des horodatages synchronisés.

11.5 Directive NIS2 de l'UE (2022/2555)

11.5.1 Article 21(2)(e) : impose des capacités de journalisation et de détection qui supposent une synchronisation temporelle exacte pour la corrélation intersystèmes et une réponse en temps utile.

11.6 DORA de l'UE (2022/2554)

11.6.1 Article 9 – Gestion des risques liés aux TIC : impose une télémétrie système exacte pour la surveillance des risques et la détection d'anomalies, laquelle dépend d'une synchronisation précise des horloges.

11.6.2 Article 10 – Continuité d'activité liée aux TIC : impose des contrôles garantissant l'intégrité du système pendant les perturbations, y compris des enregistrements d'événements alignés dans le temps.

11.7 COBIT 2019

11.7.1 DSS05.04 – Surveiller les événements de sécurité : exige l'intégrité des horodatages pour une analyse efficace des journaux et la détection des menaces.

11.7.2 MEA03 – Surveiller, évaluer et apprécier la conformité : la synchronisation temporelle contribue à l'exactitude des audits de conformité et des cycles de reporting.