					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P22S					Titre du document : **Politique de journalisation et de surveillance**							
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**

Mentions légales (droits d'auteur et restrictions d'utilisation)

(C) 2025 Clarysec LLC. All rights reserved.

Le présent document est la propriété intellectuelle de Clarysec LLC. Aucune partie de ce document ne peut être copiée, réutilisée, distribuée ou modifiée à des fins commerciales ou de mise en œuvre sans autorisation écrite expresse préalable.

Toute utilisation non autorisée est strictement interdite et peut entraîner des poursuites judiciaires.

Pour toute demande de licence, contactez : info@clarysec.com

Alignement sur les normes et réglementations

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	Clause 8	Contrôles opérationnels, y compris la journalisation
ISO/IEC 27002:2022	Mesures 8.15, 8.16, 8.17	Journalisation des événements, protection des journaux et surveillance
NIST SP 800-53 Rev.5	AU-2 à AU-12, SI-4	Contenu et revue des journaux d'audit, conservation, détection d'anomalies, alertes
RGPD	Articles 5(1)(f), 32, 33	Confidentialité et intégrité des données, mesures techniques et notification des violations
NIS2	Articles 21(2)(d), 23	Mécanismes de journalisation pour la détection des anomalies et signalement des incidents sous 24 heures
DORA	Articles 10, 15	Résilience opérationnelle numérique, surveillance et journalisation des prestataires de services
COBIT 2019	DSS01.03, DSS05.02	Traçabilité des activités et protection par la journalisation et la surveillance

1. Objet

1.1 La présente politique définit les contrôles obligatoires de journalisation et de surveillance afin d'assurer la sécurité, la responsabilité et l'intégrité opérationnelle des systèmes d'information de l'organisation.

1.2 Elle définit les types d'événements devant être journalisés, les modalités de stockage et de revue des journaux, ainsi que les responsabilités du personnel et des prestataires de services.

1.3 La journalisation et la surveillance soutiennent la détection des menaces, la conformité réglementaire, la réponse aux incidents et l'analyse forensique.

1.4 La présente politique permet à l'organisation de satisfaire aux exigences de contrôle opérationnel de l'ISO/IEC 27001 et contribue à la préparation continue aux audits, à la confiance des clients et à la conformité au RGPD, à NIS2 et à DORA.

2. Champ d'application

2.1 La présente politique s'applique à tous les systèmes et à tous les utilisateurs au sein de l'organisation, y compris :

2.1.1 les postes de travail, ordinateurs portables, serveurs, pare-feu, commutateurs, routeurs et points d'accès sans fil ;

2.1.2 les services cloud utilisés pour les activités de l'entreprise (par exemple : messagerie, stockage de fichiers, sauvegardes, outils de collaboration) ;

2.1.3 les fonctions de journalisation des logiciels antivirus, des applications, des systèmes d'exploitation et des équipements réseau ;

2.1.4 tous les employés, prestataires et prestataires de services managés (MSP) qui utilisent ou administrent les systèmes ;

2.1.5 tout lieu où les systèmes d'information de l'entreprise sont utilisés, y compris les environnements distants, hybrides ou BYOD.

2.2 La politique s'applique également aux journaux générés par des services tiers lorsque l'organisation dispose d'un accès d'administration ou de droits d'audit contractuels.

3. Objectifs

3.1 Assurer la journalisation des activités système, y compris l'authentification, les modifications de configuration, l'accès aux données sensibles et les alertes de sécurité.

3.2 Maintenir des journaux sécurisés et exacts afin de détecter les écarts à la politique, les erreurs système ou les actions non autorisées.

3.3 Permettre une revue rapide des journaux lors des incidents, des investigations et des audits.

3.4 Soutenir la synchronisation horaire afin de garantir l'intégrité et la corrélation des données de journalisation.

3.5 Protéger les journaux contre l'altération, la perte ou la suppression prématurée.

3.6 Respecter les obligations légales et réglementaires en matière de responsabilité des systèmes, de traçabilité et de réponse aux violations.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 approuve la présente politique et veille à sa mise en œuvre sur l'ensemble des systèmes métier ;

4.1.2 examine les alertes de gravité élevée et les constats d'audit critiques remontés par les fonctions informatiques ou de protection des données ;

4.1.3 approuve les dérogations lorsque la journalisation ou la conservation ne peuvent pas être mises en œuvre techniquement.

4.2 Prestataire de support informatique / fonction informatique interne

4.2.1 met en œuvre et configure la journalisation pour les systèmes d'exploitation, les équipements réseau, les outils antivirus et les applications critiques ;

4.2.2 veille à ce que les journaux soient conservés, sauvegardés et protégés contre toute altération ;

4.2.3 effectue la revue des journaux selon une fréquence définie et enquête sur les activités suspectes ou non autorisées ;

4.2.4 maintient des mécanismes d'alerte permettant de signaler les comportements anormaux ou les indicateurs d'intrusion.

[... 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 annuelle

9.1.1 La présente politique doit faire l'objet d'une revue au moins annuelle par le Directeur général, avec l'appui du prestataire de support informatique et du Coordinateur à la protection des données.

9.2 Déclencheurs de revue

9.2.1 Des revues non planifiées doivent être réalisées en réponse à :

9.2.1.1 des constats liés aux journaux issus d'audits internes ou externes ;

9.2.1.2 des incidents de sécurité pour lesquels les journaux étaient absents, corrompus ou insuffisants ;

9.2.1.3 des changements significatifs de l'infrastructure informatique (par exemple : migration vers des plateformes cloud de journalisation) ;

9.2.1.4 des mises à jour des obligations légales ou réglementaires (par exemple : RGPD, NIS2, DORA).

9.3 Gestion des versions

9.3.1 Toutes les modifications apportées à la présente politique doivent être consignées avec le numéro de version, la date et un résumé des modifications.

9.3.2 Les versions précédentes doivent être archivées et conservées pendant au moins 3 ans.

9.3.3 Les politiques mises à jour doivent être communiquées aux parties prenantes concernées, en particulier à celles disposant d'un accès au niveau système.

10. Politiques associées et articulations

10.1 La présente politique soutient directement les politiques PME de sécurité de l'information suivantes et s'articule avec elles :

10.1.1 P17S – Politique de protection des données et de la vie privée : veille à ce que les données de journalisation contenant des données à caractère personnel soient gérées avec des garanties d'intégrité, de conservation et d'accès conformes aux exigences du RGPD.

10.1.2 P21S – Politique de sécurité réseau : fournit le socle nécessaire à la collecte des journaux relatifs aux pare-feu, aux accès sans fil, aux VPN et à la surveillance de la segmentation.

10.1.3 P24S – Politique de développement sécurisé : veille à ce que les journaux applicatifs (par exemple : tentatives de connexion, erreurs et exceptions) soient intégrés dès la conception et dans l'exploitation des logiciels.

10.1.4 P30S – Politique de réponse aux incidents : s'appuie sur des données de journalisation exactes et complètes pour détecter, analyser et traiter les événements de sécurité de l'information.

10.1.5 P23S – Politique de synchronisation horaire : garantit des horodatages cohérents et traçables sur l'ensemble des systèmes, permettant la corrélation des journaux lors des investigations.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – exige la mise en œuvre de contrôles opérationnels pour atténuer les risques liés à la sécurité de l'information, y compris la journalisation.

11.2 ISO/IEC 27002

11.2.1 Mesure 8.15 – exige la journalisation des événements afin de soutenir la détection d'anomalies et la responsabilité.

11.2.2 Mesure 8.16 – exige la protection des journaux contre l'altération et l'accès non autorisé.

11.2.3 Mesure 8.17 – exige la surveillance des systèmes pour détecter les activités inhabituelles et confirmer l'efficacité des contrôles de surveillance.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 à AU-12 – couvrent le contenu des journaux d'audit, leur revue, leur conservation et l'alerte automatisée.

11.3.2 SI-4 – exige la détection des anomalies système et le signalement des événements suspects.

11.4 RGPD

11.4.1 Article 5(1)(f) – exige l'intégrité et la confidentialité des données à caractère personnel, ce qui inclut la journalisation des accès.

11.4.2 Article 32 – impose des mesures techniques et organisationnelles pour assurer la sécurité, y compris la journalisation et la surveillance.

11.4.3 Article 33 – exige une notification rapide des violations, appuyée par des journaux permettant une analyse de la cause racine.

11.5 Directive NIS2

11.5.1 Article 21(2)(d) – exige des mécanismes de journalisation permettant de détecter les anomalies et d'apporter un appui lors des investigations sur incident.

11.5.2 Article 23 – impose le signalement des incidents dans un délai de 24 heures, ce qui dépend de données de journalisation exactes et disponibles en temps utile.

11.6 DORA

11.6.1 Article 10 – exige la résilience opérationnelle numérique, y compris la traçabilité des incidents liés aux TIC au moyen de la journalisation.

11.6.2 Article 15 – impose la surveillance des prestataires de services, y compris l'accès aux journaux et les droits de revue.

11.7 COBIT 2019

11.7.1 DSS01.03 – exige la traçabilité de l'activité des systèmes au moyen de la journalisation et de la surveillance.

11.7.2 DSS05.02 – traite la journalisation comme un contrôle clé de protection contre les logiciels malveillants et toute autre activité non autorisée.