					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P22					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**

1. Objet

1.1 La présente politique a pour objet d'établir des exigences claires et opposables relatives à la génération, à la protection, à la revue et à l'analyse des journaux consignant les principaux événements système et de sécurité au sein de l'environnement informatique de l'organisation.

1.2 La journalisation et la surveillance sont essentielles à la détection des anomalies, à la réponse aux menaces, à l'investigation forensique, à la préparation des audits et à la conformité réglementaire. La présente politique impose que tous les événements générés par les systèmes soient correctement journalisés, conservés et corrélés, avec un niveau de précision reposant sur des journaux horodatés au moyen de sources temporelles synchronisées.

1.3 La présente politique est indispensable au soutien de la clause 8.1 de l'ISO/IEC 27001 ainsi que des mesures 8.15 (journalisation), 8.16 (surveillance) et 8.17 (synchronisation des horloges) de l'annexe A, et répond directement aux obligations réglementaires applicables au titre du RGPD, de NIS2, de DORA et de COBIT 2019.

2. Champ d’application

2.1 La présente politique s'applique à tous les systèmes, services et environnements qui stockent, traitent ou transmettent des données couvertes par le système de management de la sécurité de l'information (SMSI), y compris :

2.1.1 les infrastructures sur site, les services cloud (par exemple IaaS, PaaS, SaaS) et les environnements hybrides ;

2.1.2 les systèmes d'exploitation, les bases de données, les applications et les équipements réseau ;

2.1.3 les systèmes de sécurité tels que les SIEM, les pare-feu, les plateformes EDR, les concentrateurs VPN et les fournisseurs d'identité.

2.2 Les parties prenantes suivantes entrent dans le champ d’application :

2.2.1 les utilisateurs internes disposant de privilèges système ou administratifs ;

2.2.2 le personnel en charge des opérations d'infrastructure et des opérations informatiques ;

2.2.3 le centre des opérations de sécurité (SOC) et les équipes de détection des menaces ;

2.2.4 les développeurs logiciels et les propriétaires d'applications ;

2.2.5 les prestataires de services tiers qui administrent des systèmes générant des journaux.

3. Objectifs

3.1 Veiller à ce que tous les systèmes critiques génèrent des journaux d'événements de sécurité et des enregistrements d'activité système, conservés conformément aux exigences réglementaires, légales et contractuelles.

3.2 Définir les types d'événements minimaux et le contenu des journaux requis pour détecter les activités non autorisées, assurer la traçabilité des actions des utilisateurs et soutenir les investigations forensiques.

3.3 Imposer des mesures de protection afin d'empêcher l'altération des journaux, leur suppression non autorisée ou tout accès non maîtrisé aux données de journalisation.

3.4 Mettre en place des dispositifs centralisés de journalisation et d'alerte (par exemple SIEM) afin d'agréger, de corréler et d'escalader les activités suspectes en quasi temps réel.

3.5 Garantir la synchronisation des horloges système afin de permettre une corrélation fiable entre systèmes et l'analyse des incidents.

3.6 Permettre l'amélioration continue et la conformité en articulant la surveillance des journaux avec les processus d'audit, de gestion des risques et de gestion des incidents.

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 le niveau de risque de l'organisation, les exigences d'audit et les obligations du SMSI.

4.1.2 Approuve le périmètre de journalisation des systèmes réglementés ou à haut risque et supervise l'établissement des rapports de conformité.

4.2 Responsable du centre des opérations de sécurité (SOC)

4.2.1 Exploite et maintient les plateformes centralisées de gestion des journaux (par exemple SIEM).

4.2.2 Définit les règles d'agrégation des journaux, les seuils d'alerte et les circuits d'escalade pour le tri des incidents.

4.2.3 Revoit les rapports quotidiens et veille à ce que les anomalies soient analysées, documentées et escaladées selon les besoins.

[... 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 être revue annuellement, ou plus tôt en réponse à :

9.1.1 des changements majeurs dans l'architecture des systèmes ou l'infrastructure de journalisation (par exemple migration du SIEM) ;

9.1.2 des révisions des exigences réglementaires en matière de journalisation (par exemple exigences de journalisation NIS2, DORA) ;

9.1.3 des constats issus d'audits ou de revues post-incident ;

9.1.4 des menaces émergentes nécessitant un renforcement de la surveillance (par exemple menace interne, compromission de la chaîne d'approvisionnement).

9.2 Le processus de revue doit être piloté par le responsable du centre des opérations de sécurité (SOC), en coordination avec le RSSI, la gestion des risques, la conformité et les équipes d'infrastructure informatique.

9.3 Les changements approuvés doivent faire l'objet d'une gestion de versions dans le registre de contrôle documentaire du SMSI et être communiqués :

9.3.1 à toutes les parties prenantes responsables de la maintenance des systèmes de journalisation ;

9.3.2 aux propriétaires d'applications et de systèmes ;

9.3.3 aux prestataires tiers ayant des obligations de télémétrie ou d'intégration au SIEM.

9.4 Toutes les versions remplacées doivent être archivées de manière sécurisée, avec un accès limité aux dépositaires autorisés du SMSI à des fins d'audit et juridiques.

10. Politiques associées et articulations

10.1 P1 – Politique de sécurité de l'information. Établit l'engagement fondamental de protection des systèmes et des données, dans le cadre duquel la journalisation et la surveillance constituent des contrôles détectifs et des moyens de réponse essentiels.

10.2 P4 – Politique de contrôle d'accès. Garantit que les accès à privilèges, les connexions des utilisateurs et les événements d'autorisation sont journalisés et surveillés afin de détecter les abus ou les comportements anormaux.

10.3 P5 – Politique de gestion des changements. Impose la journalisation des changements système, des déploiements de correctifs et des mises à jour de configuration susceptibles d'introduire des risques ou des modifications non autorisées.

10.4 P21 – Politique de sécurité réseau. Exige la journalisation au niveau réseau (par exemple journaux de pare-feu, alertes IDS/IPS, activité VPN) et l'intégration avec le SIEM afin d'assurer la visibilité sur les anomalies de trafic et la protection du périmètre.

10.5 P23 – Politique de synchronisation temporelle. Implique la cohérence des horloges entre les systèmes, indispensable à une journalisation fiable et à la corrélation des événements de sécurité dans plusieurs environnements.

10.6 P30 – Politique de réponse aux incidents. S'appuie sur les données de journalisation et les mécanismes d'alerte pour identifier, investiguer et traiter les incidents de sécurité, tout en préservant les artefacts forensiques en vue de la revue post-incident.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Planification et maîtrise opérationnelles : exige des contrôles permettant de surveiller les opérations et de se prémunir contre les accès non autorisés et l'usage abusif des systèmes.

11.2 ISO/IEC 27002:2022 – Mesures 8.15, 8.16, 8

11.2.1 Définit des exigences détaillées en matière de journalisation, notamment les événements à consigner, les modalités de protection et d'analyse des journaux, ainsi que les moyens d'assurer la fiabilité des horodatages entre systèmes.

11.3 NIST SP 800-53 Rev.

11.3.1 AU-2 à AU-12 : couvre la sélection des événements, la journalisation, la protection, la revue d'audit, la réponse aux défaillances d'audit et la conservation des enregistrements d'audit.

11.3.2 SI-4 – Surveillance des systèmes : exige une surveillance active des systèmes avec des alertes fondées sur des activités anormales.

11.3.3 SC-45 – Synchronisation temporelle des systèmes : renforce l'exactitude temporelle pour la traçabilité des événements et la corrélation des incidents.

11.4 RGPD de l'UE (2016/679)

11.4.1 Article 32 – Sécurité du traitement : exige des mesures techniques telles que la journalisation et la surveillance afin d'assurer la sécurité et la responsabilité, en particulier pour l'accès aux données à caractère personnel.

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

11.5.1 Article 21(2)(e) : impose des systèmes de journalisation et de surveillance des événements pour une détection et une réponse rapides aux incidents de sécurité.

11.6 DORA de l'UE (2022/2554)

11.6.1 Article 9 – Gestion des risques liés aux TIC : exige des mécanismes permettant de détecter les activités anormales, de journaliser les incidents et de conserver des données forensiques.

11.6.2 Article 11 – Tests des plans de continuité d'activité TIC : met l'accent sur la continuité de la surveillance et la validation de la disponibilité des journaux pendant les perturbations opérationnelles.

11.7 COBIT 2019

11.7.1 DSS01.05 – Gérer les journaux de sécurité : exige la mise en œuvre de capacités de journalisation pour toutes les infrastructures critiques.

11.7.2 DSS05.04 – Surveiller les événements de sécurité : impose la surveillance et l'analyse en temps réel des journaux pour détecter les événements et y répondre.

11.7.3 MEA03 – Surveiller, évaluer et apprécier la conformité : exige une revue régulière des pratiques de journalisation et leur alignement avec les objectifs de contrôle.