					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P31S					Titre du document : **Politique de collecte des éléments de preuve et d'investigation forensique**							
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	Clauses 6.1, 6.3, 8	Planification fondée sur les risques, actions d'amélioration et contrôles opérationnels pour l'intégrité des éléments de preuve
ISO/IEC 27002:2022	Mesures 5.24–5.27	Encadre le traitement sécurisé, les revues post-incident et les améliorations fondées sur les éléments de preuve
ISO/IEC 27035-3:2016	Clauses 6.3, 6.4, 7	Garantit une planification appropriée, une collecte licite et un traitement sécurisé des éléments de preuve numériques, avec documentation de la chaîne de conservation
NIST SP 800-53 Rév. 5	IR-07, IR-08, AU-09, AU-12, PE-18	Préparation forensique, protection des journaux d'audit et intégration efficace dans la réponse aux incidents
RGPD de l'UE	Articles 33, 34	Documentation et traçabilité des violations de données à caractère personnel
NIS2 de l'UE	Article 23	Signalement traçable des incidents et traitement sécurisé des éléments de preuve
DORA de l'UE	Article 17(1), 17(2)	Garantit la collecte, le stockage et la conservation des éléments de preuve pour les incidents liés aux TIC, la recevabilité forensique et les demandes des autorités de régulation
COBIT 2019	DSS05.06, DSS05.07	Journalisation fiable et traitement structuré des éléments de preuve pour des investigations sûres et auditables

1. Objet

1.1. La présente politique définit les modalités selon lesquelles l'organisation traite les éléments de preuve numériques liés aux incidents de sécurité, aux violations de données ou aux investigations internes. Elle exige que les éléments de preuve soient collectés, stockés et conservés d'une manière juridiquement recevable et conforme aux exigences d'audit, afin de soutenir à la fois la prise de décision interne et, le cas échéant, les suites externes.

1.2. La politique permet aux petites organisations de protéger l'intégrité des journaux, des fichiers et des images système tout en démontrant une diligence raisonnable au regard de l'ISO/IEC 27001, du RGPD et des normes associées.

1.3. Elle soutient la préparation forensique sans exiger de ressources techniques avancées ni d'équipe informatique à temps plein, en définissant clairement les responsabilités, les processus et les exigences de conservation.

2. Champ d'application

2.1. La présente politique s'applique à :

2.1.1. Tous les employés, prestataires informatiques et consultants externes intervenant dans la réponse aux incidents, l'investigation ou l'analyse des violations

2.1.2. Tous les systèmes de l'entreprise, y compris les ordinateurs portables, appareils mobiles, serveurs, comptes de messagerie, plateformes SaaS et espaces de stockage cloud (par exemple Microsoft 365, Google Workspace)

2.1.3. Tout événement nécessitant des éléments de preuve dans le cadre d'une mesure disciplinaire interne, d'une défense juridique, d'une demande d'indemnisation auprès d'un assureur ou d'un échange avec une autorité de régulation

2.2. Elle couvre les événements avérés comme suspectés impliquant :

2.2.1. Une fuite de données

2.2.2. Une menace interne ou un usage abusif

2.2.3. Des violations de sécurité (par exemple logiciels malveillants, accès non autorisé)

2.2.4. Des réclamations clients nécessitant une validation numérique

2.2.5. Des demandes d'information émanant d'une autorité de régulation ou des forces de l'ordre

3. Objectifs

3.1. Garantir que tous les éléments de preuve sont collectés et traités de manière à préserver leur intégrité, leur authenticité et la chaîne de conservation.

3.2. Prévenir toute modification accidentelle, suppression ou mauvaise manipulation des journaux, fichiers ou images système susceptibles d'être nécessaires à une investigation.

3.3. Fournir une approche cohérente et auditable de la gestion des éléments de preuve, répondant aux attentes légales et réglementaires (par exemple notification de violation au titre du RGPD, traçabilité au titre de NIS2).

3.4. Définir des rôles et responsabilités clairs afin d'assurer une collecte rapide, sécurisée et juridiquement conforme des éléments de preuve lors d'incidents de sécurité.

3.5. Soutenir un niveau de préparation forensique adapté aux PME tout en limitant la complexité et en évitant les perturbations des activités courantes.

4. Rôles et responsabilités

4.1. Directeur général (DG)

4.1.1. Approuve toute investigation formelle nécessitant une collecte d'éléments de preuve.

4.1.2. Examine et valide les rapports d'incident impliquant d'éventuelles suites juridiques ou disciplinaires.

4.1.3. Décide s'il y a lieu de notifier le conseil juridique externe ou les autorités de régulation.

4.1.4. Veille à ce que la politique fasse l'objet d'une revue et d'une mise à jour régulières.

4.2. Prestataire informatique / administrateur système

4.2.1. Collecte et conserve les éléments de preuve numériques conformément à des procédures sécurisées.

4.2.2. Documente les horodatages, les détails du système et les étapes de traitement.

4.2.3. Sécurise l'ensemble des éléments collectés dans un emplacement protégé.

4.2.4. Apporte son concours à l'analyse forensique si nécessaire.

[... 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 de la politique

9.1.1. La présente politique doit faire l'objet d'une revue au moins une fois tous les 12 mois par le Directeur général (DG) afin de confirmer :

9.1.1.1. La conformité aux mesures de l'Annexe A de l'ISO/IEC 27001

9.1.1.2. Le maintien de sa pertinence au regard des plateformes numériques et des services informatiques en vigueur

9.1.1.3. L'adéquation des procédures de journalisation, de conservation des éléments de preuve et de préparation forensique

9.2. Déclencheurs de revue de la politique

9.2.1. La politique doit également être revue et mise à jour après :

9.2.1.1. Tout incident majeur nécessitant une collecte d'éléments de preuve

9.2.1.2. Un audit non concluant ou une demande réglementaire dans le cadre desquels l'intégrité des éléments de preuve a été remise en question

9.2.1.3. L'adoption de nouveaux outils ou procédures pour la réponse aux incidents ou la surveillance des systèmes

9.2.1.4. Des évolutions juridiques (par exemple mise à jour des orientations relatives au RGPD ou à NIS2)

9.3. Approbation et diffusion des modifications

9.3.1. Toutes les modifications doivent être examinées et approuvées par le DG

9.3.2. La version mise à jour doit être partagée avec :

9.3.2.1. Les prestataires informatiques et consultants impliqués dans les investigations

9.3.2.2. Tout membre du personnel ayant des responsabilités d'administration système

9.3.3. Une copie mise à jour doit être conservée dans les archives des politiques de l'entreprise et communiquée aux auditeurs sur demande

10. Politiques associées et articulations

10.1. La présente politique est interdépendante avec les politiques suivantes, alignées sur le contexte des PME :

10.1.1. P2S – Politique relative aux rôles et responsabilités de gouvernance : établit l'autorité en matière d'investigations sur incident, de décisions relatives aux éléments de preuve et d'escalade juridique.

10.1.2. P4S – Politique de contrôle d'accès : garantit que seul le personnel autorisé peut accéder aux systèmes sensibles et aux journaux pendant les investigations.

10.1.3. P22S – Politique de journalisation et de surveillance : fournit les données brutes utilisées comme éléments de preuve forensiques et définit les exigences de conservation, de contrôle d'accès et de journalisation.

10.1.4. P30S – Politique de réponse aux incidents : déclenche le besoin de collecte des éléments de preuve et définit le déroulement opérationnel conduisant à leur conservation forensique.

10.1.5. P17S – Politique de protection des données et de la vie privée : garantit que toutes les données à caractère personnel collectées comme éléments de preuve sont traitées licitement au titre du RGPD et des réglementations associées.

10.2. Ces politiques s'articulent pour soutenir la défendabilité juridique, l'intégrité des investigations et la capacité à répondre pleinement à un audit ISO/IEC 27001:2022.

11. Normes et référentiels de référence

11.1. ISO/IEC 27001

11.1.1. Clause 6.1 – La planification fondée sur les risques inclut la préparation à la réponse et les procédures relatives aux éléments de preuve.

11.1.2. Clause 6.3 – Soutient les actions d'amélioration fondées sur les éléments de preuve issus des incidents.

11.1.3. Clause 8.1 – Exige des contrôles opérationnels pour l'intégrité des éléments de preuve.

11.2. ISO/IEC 27002

11.2.1. Mesures 5.24–5.27 – Encadrent le traitement sécurisé, les revues post-incident et les améliorations fondées sur les éléments de preuve.

11.3. ISO/IEC 27035-3

11.3.1. Clauses 6.3, 6.4 et 7.3 – visent à garantir une planification appropriée, une collecte licite et un traitement sécurisé des éléments de preuve numériques pendant la réponse aux incidents, y compris leur conservation et la documentation de la chaîne de conservation.

11.4. NIST SP 800-53 Rév. 5

11.4.1. IR-07, IR-08, AU-09 et AU-12 – garantissent la préparation forensique, la protection des journaux d'audit et l'intégration efficace de la collecte des éléments de preuve dans le cycle de vie de la réponse aux incidents

11.5. NIST SP 800-86

11.5.1. Définit les bonnes pratiques pour l'acquisition, l'analyse et la protection des éléments de preuve numériques dans le cadre de la réponse aux incidents.

11.6. RGPD de l'UE

11.6.1. Articles 33–34 – imposent la documentation et la traçabilité des incidents et des éléments de preuve lors du signalement des violations de données à caractère personnel.

11.7. Directive NIS2 de l'UE (2022/2555)

11.7.1. Article 23 – exige un signalement traçable des incidents et un traitement sécurisé des éléments de preuve pour les entités essentielles et importantes.

11.8. DORA de l'UE

11.8.1. Article 17(1) – exige que les éléments de preuve liés aux incidents TIC soient collectés et stockés d'une manière permettant de soutenir les investigations forensiques.

11.8.2. Article 17(2) – exige que les entités financières conservent toutes les données et tous les journaux pertinents associés aux événements de sécurité, en cohérence avec les exigences forensiques et les demandes des autorités de régulation.

11.9. COBIT 2019

11.9.1. DSS05.06 – Surveiller, détecter et signaler les incidents : met l'accent sur une journalisation fiable au service des investigations.

11.9.2. DSS05.07 – Investiguer et traiter les incidents : exige un traitement structuré des éléments de preuve pour permettre des investigations sûres et auditables.