					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P31					Titre du document : **Politique de collecte des éléments de preuve et d'investigation numérique**							
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	Mesures 5.25–5.27, 8.27	
ISO/IEC 27035:2016	Parties 1 et 3	
NIST SP 800-53 Rev.5	IR-1 à IR-9, AU-6, PL-2	
NIST SP 800-101 Rev.1	Investigation numérique des appareils mobiles	Investigation numérique mobile/des supports
NIST SP 800-86	Intégration des techniques d'investigation numérique	Intégration des techniques d'investigation numérique dans la réponse aux incidents
RGPD de l'UE	Articles 5, 33–34	
NIS2 de l'UE	Article 23(1)–(4)	
DORA de l'UE	Article 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05	

1. Objet

1.1 La présente politique établit un cadre structuré et juridiquement défendable pour l'identification, la collecte, la conservation, l'analyse et l'élimination des éléments de preuve numériques lors d'incidents de sécurité avérés ou suspectés.

1.2 Elle impose que les processus de préparation à l'investigation numérique et de gestion des éléments de preuve :

1.2.1 préservent l’intégrité probatoire et la chaîne de conservation

1.2.2 soutiennent les investigations internes, les procédures judiciaires ou les obligations d'information réglementaires

1.2.3 soient alignés sur les normes d'investigation numérique reconnues au niveau international et sur les critères de recevabilité juridique

1.3 La politique soutient l'engagement de l'organisation en faveur d'une réponse proactive aux incidents, de la conformité juridique et de la transparence de la gouvernance, tout en limitant les perturbations opérationnelles.

2. Champ d’application

2.1 La présente politique s'applique :

2.1.1 à l'ensemble des employés, prestataires, fournisseurs et prestataires de services intervenant dans l'administration des systèmes, la gestion des incidents ou les activités d'investigation

2.1.2 à tous les postes de travail, serveurs, applications, réseaux et plateformes cloud relevant du contrôle de l'organisation ou de sa responsabilité contractuelle

2.1.3 à tout incident ou événement nécessitant la gestion d’éléments de preuve, y compris :

2.1.3.1 les menaces internes, violations de données ou enquêtes pour fraude

2.1.3.2 l'usage abusif des systèmes ou des identifiants d’authentification

2.1.3.3 les incidents affectant les systèmes de technologies opérationnelles (OT) ou les systèmes de contrôle industriel

2.1.3.4 les manquements à la sécurité physique impliquant des actifs numériques

2.2 La politique encadre également toute interaction avec des prestataires spécialisés en investigation numérique ou les autorités répressives dans le cadre d'une escalade juridique ou d'une procédure réglementaire.

3. Objectifs

3.1 Permettre une acquisition rapide, sécurisée et conforme à la politique des éléments de preuve lors d'événements de sécurité ou d'investigations.

3.2 Préserver l'intégrité, l'authenticité et la recevabilité des éléments de preuve numériques collectés au moyen d'un contrôle strict des accès, de la journalisation et de procédures de vérification.

3.3 Garantir que toutes les activités d'investigation numérique sont coordonnées avec les obligations juridiques et réglementaires, y compris en matière de protection des données, de droit du travail et de restrictions applicables aux transferts internationaux.

3.4 Soutenir l'analyse post-incident, la détermination de la cause racine et l'amélioration des contrôles grâce à une production probatoire de haute qualité.

3.5 Intégrer la préparation à l'investigation numérique dans l'ensemble du système de management de la sécurité de l'information (SMSI), afin de soutenir les audits, les notifications de violation et la prise de décision de la direction.

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 ce que toutes les opérations d'investigation numérique soient juridiquement défendables, auditables et fondées sur les risques.

4.1.2 Autorise l'escalade vers des entités juridiques externes et des prestataires spécialisés en investigation numérique.

4.2 Analystes en investigation numérique / intervenants en gestion des incidents

4.2.1 Pilotent l'acquisition, la conservation et l'analyse technique des éléments de preuve.

4.2.2 Veillent à ce que la chaîne de conservation soit correctement documentée et maintenue.

4.2.3 Documentent l'ensemble des actions, constats et paramètres des outils utilisés pendant les investigations.

[... 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 au moins annuelle et être mise à jour si nécessaire afin de refléter :

9.1.1 les évolutions législatives, réglementaires ou jurisprudentielles affectant les procédures d'investigation numérique ou le traitement des données

9.1.2 les mises à jour des normes d'investigation numérique ou des jeux d'outils reconnus par le secteur

9.1.3 les enseignements tirés des revues post-incident, des litiges ou des constats d'audit

9.1.4 les évolutions technologiques des plateformes, équipements ou systèmes faisant l'objet d'une investigation

9.2 Le processus de revue relève du RSSI et doit inclure la consultation des parties suivantes :

9.2.1 juridique et conformité

9.2.2 délégué à la protection des données (DPD)

9.2.3 équipes des opérations de sécurité et d'investigation numérique

9.2.4 audit interne

9.3 Toutes les révisions doivent être :

9.3.1 soumises à la gestion des versions et conservées dans le référentiel des politiques

9.3.2 communiquées aux parties prenantes concernées, y compris les équipes d'investigation numérique et de réponse

9.3.3 accompagnées de mises à jour des procédures opérationnelles et des supports de formation pertinents

9.4 Des revues intermédiaires doivent être déclenchées après tout incident critique impliquant une mauvaise gestion des éléments de preuve, une défaillance de la chaîne de conservation ou des problèmes de recevabilité juridique.

10. Politiques associées et articulations

10.1 La présente politique est alignée sur les politiques organisationnelles suivantes et soutenue par celles-ci :

10.1.1 P1 – Politique de sécurité de l'information : établit le cadre de référence pour l'investigation, le contrôle des éléments de preuve et la conformité aux lois applicables.

10.1.2 P5 – Politique de gestion des changements : garantit que les systèmes faisant l'objet d'une investigation ne sont pas modifiés pendant les processus d'investigation numérique en cours.

10.1.3 P14 – Politique de conservation et d'élimination des données : encadre l'élimination sécurisée et les durées de conservation applicables aux éléments de preuve et aux données liées aux dossiers.

10.1.4 P18 – Politique relative aux contrôles cryptographiques : définit les exigences de chiffrement applicables au stockage et au transfert de données sensibles ou probatoires.

10.1.5 P22 – Politique de journalisation et de surveillance : garantit la disponibilité des journaux d'événements et de la télémétrie pour la collecte des éléments de preuve et la corrélation d'investigation numérique.

10.1.6 P30 – Politique de réponse aux incidents : définit le triage des incidents et les circuits d'escalade déclenchant les procédures d'investigation numérique.

10.1.7 P33 – Politique d'audit et de surveillance de la conformité : valide le respect des protocoles d'investigation numérique et des exigences de chaîne de conservation au moyen d'audits réguliers.

11. Normes et référentiels de référence

11.1 La présente politique est alignée sur les normes internationales relatives aux investigations numériques et à la gestion des incidents, afin de garantir l'intégrité des éléments de preuve, la défendabilité juridique et la conformité dans des juridictions multiples.

11.2 ISO/IEC 27001

11.2.1 Clause 8.1 – Soutient le contrôle opérationnel de la préparation à l'investigation numérique et des procédures relatives aux éléments de preuve.

11.3 ISO/IEC 27002

11.3.1 Annexe A Mesure 5.25 – Responsabilités relatives à la gestion des incidents : exige la définition de rôles pour le traitement des incidents de sécurité de l'information et des investigations.

11.3.2 Annexe A Mesure 5.26 – Signalement des événements de sécurité de l'information : soutient la collecte, à titre probatoire, d'éléments justificatifs liés aux événements.

11.3.3 Annexe A Mesure 5.27 – Réponse aux incidents de sécurité de l'information : impose une remédiation et une investigation structurées, fondées sur les éléments de preuve.

11.3.4 Annexe A Mesure 8.27 – Développement sécurisé et investigation numérique (le cas échéant) : traite de la protection des systèmes et des outils pendant les investigations.

11.4 ISO/IEC 27035:2016 (parties 1 et 3)

11.4.1 Décrit les principes de détection des incidents, de réponse et de préparation à l'investigation numérique, y compris la planification, la chaîne de conservation et la gestion des éléments de preuve liés aux incidents.

11.5 NIST SP 800-53 Rev.5

11.5.1 IR-1 à IR-9, AU-6, PL-2 : définit des exigences structurées pour la planification, la détection, l'analyse, le confinement et la réponse aux incidents de sécurité. Soutient la collecte et l'auditabilité des éléments de preuve (AU-6) et garantit l'alignement sur les plans de sécurité des systèmes et de protection de la vie privée (PL-2) lors des investigations numériques.

11.6 NIST SP 800-86

11.6.1 Fournit des lignes directrices sur l'intégration des processus d'investigation numérique dans le cycle de vie plus large de la réponse aux incidents et sur la préparation à l'investigation numérique.

11.7 NIST SP 800-101 Rev.1

11.7.1 Met l'accent sur les bonnes pratiques d'acquisition, de conservation et d'analyse des supports numériques et des éléments de preuve issus d'appareils mobiles de manière juridiquement défendable.

11.8 RGPD de l'UE (2016/679)

11.8.1 Article 5 – Principes relatifs au traitement des données à caractère personnel : s'applique aux éléments de preuve contenant des données personnelles ou sensibles, en imposant la minimisation et la limitation des finalités.

11.8.2 Articles 33–34 – Notification de violation de données : les données d'investigation numérique soutiennent la conformité aux obligations de notification de violation et aux processus de divulgation juridique.

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

11.9.1 Article 23 – Obligations d'information : la documentation et les constats d'investigation numérique soutiennent des rapports d'incident exacts et transmis en temps utile aux autorités compétentes.

11.10 DORA de l'UE (2022/2554)

11.10.1 Article 17 – Signalement des incidents liés aux TIC : exige des enregistrements détaillés de la cause racine et des éléments probatoires relatifs aux incidents TIC majeurs, en particulier dans le secteur financier.

11.11 COBIT 2019

11.11.1 DSS01.07 – Gérer les incidents de sécurité : impose la documentation des incidents et une rigueur d'investigation appropriée.

11.11.2 DSS05.04 – Gérer les investigations de sécurité : met l'accent sur la conservation des éléments de preuve numériques et le soutien aux actions disciplinaires et judiciaires.