					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P30S					Titre du document : **Politique de réponse aux incidents**							
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	Gestion des incidents, amélioration continue, maîtrise opérationnelle
ISO/IEC 27002:2022	Mesures 5.24, 5.25	Détection des incidents, préparation, retour d'expérience
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	Gestion et surveillance des incidents, signalement
RGPD (UE)	Article 33	Exigences de notification des violations
NIS2 (UE)	Article 23	Signalement obligatoire des cyberincidents
DORA (UE)	Article 17	Gestion des incidents liés aux TIC
COBIT 2019	DSS02, DSS04	Gestion des services et des incidents, continuité

1. Objet

1.1. La présente politique définit la manière dont l'organisation détecte, signale et traite les incidents de sécurité de l'information affectant ses systèmes numériques, ses données ou ses services.

1.2. Elle permet à l'organisation de limiter les dommages, de protéger les données des clients et de respecter les obligations réglementaires, notamment l'exigence du RGPD relative à la notification d'une violation dans un délai de 72 heures.

1.3. La politique définit clairement les responsabilités, les étapes de communication et le suivi post-incident, y compris dans les petites organisations ne disposant pas d'une équipe de sécurité dédiée.

2. Champ d’application

2.1. La présente politique s'applique à :

2.1.1. Tous les employés, prestataires et prestataires externes de services informatiques

2.1.2. Tous les systèmes et services gérés par l'entreprise, y compris les sites web, les plateformes cloud, les appareils mobiles, les ordinateurs portables et les comptes de messagerie

2.1.3. Tous les types d'incidents, y compris :

2.1.3.1. Les accès non autorisés aux données ou aux systèmes

2.1.3.2. Les infections par des logiciels malveillants ou des rançongiciels

2.1.3.3. Les tentatives de phishing ou d'ingénierie sociale

2.1.3.4. Les interruptions de service dues à une cyberattaque ou à un usage abusif

2.1.3.5. La divulgation accidentelle ou la suppression d'informations sensibles

2.1.3.6. La perte ou le vol d'équipements professionnels ou de supports de stockage

3. Objectifs

3.1. Établir un processus clair pour identifier et escalader les incidents de sécurité.

3.2. Garantir que les incidents sont signalés, consignés et traités dans des délais prédéfinis.

3.3. Permettre un confinement rapide des dommages, la restauration des données et le rétablissement des services.

3.4. Garantir que les parties concernées (par exemple, les clients, les autorités de contrôle) sont notifiées lorsque la loi l'exige.

3.5. Prévenir toute récurrence au moyen d'une analyse des causes racines, d'actions correctives et de l'amélioration de la politique.

3.6. Permettre aux PME de satisfaire aux exigences de certification ISO/IEC 27001 et de démontrer leur responsabilité lors des audits.

4. Rôles et responsabilités

4.1. Directeur général (DG)

4.1.1. Est responsable de la présente politique et veille à sa mise en œuvre.

4.1.2. Supervise les activités de réponse aux incidents et approuve les notifications aux autorités de contrôle ou aux clients.

4.1.3. Examine les rapports post-incident et veille à ce que les mises à jour de la politique soient effectuées lorsque nécessaire.

4.1.4. Peut déléguer les tâches de coordination, tout en conservant la responsabilité.

4.2. Prestataire informatique / administrateur système (interne ou externe)

4.2.1. Détecte et analyse les incidents de sécurité potentiels.

4.2.2. Met en œuvre les actions de confinement et de rétablissement (par exemple, désactivation des accès, restauration des sauvegardes).

4.2.3. Informe le DG de tout incident confirmé ou suspecté dans un délai d'une heure après sa découverte.

4.2.4. Tient un journal des incidents comportant les horodatages, l'évaluation de l'impact et les actions de réponse.

[... 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 planifiée

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 garantir :

9.1.1.1. L'alignement sur les mesures d'ISO/IEC 27001:2022

9.1.1.2. La prise en compte des nouvelles menaces, des nouveaux risques et des nouveaux incidents

9.1.1.3. Le maintien de la conformité avec les obligations légales et contractuelles (par exemple, RGPD, DORA)

9.2. Événements déclencheurs

9.2.1. La politique doit également faire l'objet d'une revue et d'une mise à jour après :

9.2.1.1. Tout incident de gravité élevée ou toute notification réglementaire

9.2.1.2. L'introduction de nouvelles infrastructures informatiques ou de changements de système

9.2.1.3. Toute modification des exigences légales relatives aux violations de sécurité

9.3. Documentation de revue et diffusion

9.3.1. Toutes les revues et modifications doivent être documentées dans le journal des modifications de la politique

9.3.2. Les versions mises à jour doivent être diffusées à tous les employés, fournisseurs et prestataires informatiques impliqués dans la sécurité ou l'exploitation des systèmes

9.3.3. Les éléments de preuve de la sensibilisation du personnel (par exemple, comptes rendus de réunion ou confirmations par courriel) doivent être conservés afin de démontrer la conformité en audit

10. Politiques associées et articulations

10.1. La présente politique doit être appliquée en articulation avec les politiques PME suivantes :

10.1.1. P1S – Politique de sécurité de l'information : définit les exigences générales de maintien de la confidentialité, de l'intégrité et de la disponibilité pendant les opérations, y compris la gestion des incidents.

10.1.2. P2S – Politique relative aux rôles et responsabilités de gouvernance : établit les structures d'autorité et de responsabilité pour la détection, le signalement et l'escalade des incidents.

10.1.3. P4S – Politique de contrôle d’accès : permet la révocation immédiate des droits d’accès dans le cadre des actions de réponse aux incidents.

10.1.4. P8S – Politique de sensibilisation et de formation à la sécurité de l'information : garantit que tous les employés sont en mesure d'identifier et de signaler efficacement les incidents de sécurité.

10.1.5. P17S – Politique de protection des données et de la vie privée : encadre les procédures légales de notification des violations au titre du RGPD et contribue à la conformité réglementaire lors des incidents.

10.1.6. P22S – Politique de journalisation et de surveillance : fournit les outils et la visibilité nécessaires pour détecter, analyser et auditer les événements de sécurité.

10.1.7. P31S – Politique d'investigation forensique : soutient l'investigation et la recevabilité juridique des actions liées aux incidents en encadrant la gestion appropriée des éléments de preuve.

10.2. Ensemble, ces politiques établissent le cadre opérationnel de la PME pour détecter, traiter et rétablir les activités après un incident de sécurité de l'information.

11. Normes et référentiels de référence

11.1. ISO/IEC 27001

11.1.1. Clause 6.1 – Exige une planification du traitement des risques, y compris la préparation aux incidents.

11.1.2. Clause 6.3 – Soutient l'amélioration continue grâce aux enseignements tirés des événements de sécurité.

11.1.3. Clause 8.1 – Met l'accent sur la maîtrise opérationnelle pour gérer les incidents et les perturbations.

11.2. ISO/IEC 27002

11.2.1. Mesure 5.24 – Exige une approche structurée pour le signalement, l'évaluation et le traitement des incidents de sécurité de l'information.

11.2.2. Mesure 5.25 – Met l'accent sur le retour d'expérience afin d'améliorer la préparation future et la résilience des systèmes.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – Définit les procédures de gestion des incidents, y compris le confinement et le rétablissement.

11.3.2. IR-5 – Établit les exigences relatives à la surveillance et à l'analyse des incidents.

11.3.3. IR-6 – Impose des protocoles de signalement des incidents en interne et en externe.

11.4. RGPD (UE)

11.4.1. Article 33 – Exige la notification des violations de données à caractère personnel aux autorités de contrôle dans un délai de 72 heures, avec des précisions sur le périmètre et les mesures d'atténuation.

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

11.5.1. Article 23 – Exige des entités essentielles et importantes qu'elles notifient les incidents significatifs aux autorités compétentes au moyen de formats de signalement normalisés.

11.6. Règlement DORA de l'UE (2022/2554)

11.6.1. Article 17 – Exige des entités financières qu'elles classent, signalent et suivent les incidents et perturbations liés aux TIC.

11.7. COBIT 2019

11.7.1. DSS02 – Gérer les demandes de service et les incidents : fournit un cadre pour une gestion efficace des incidents opérationnels et de sécurité, conforme aux objectifs de gouvernance.

11.7.2. DSS04 – Gérer la continuité : articule la réponse aux incidents avec des stratégies plus larges de continuité et de reprise.