					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P19S					Titre du document : **Politique de gestion des vulnérabilités et des correctifs**							
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 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
NIS2 (UE)	Articles 21(2)(d), 21(2)(e)	
DORA (UE)	Articles 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
RGPD (UE)	Article 32(1)(b)	

1. Objet

1.1 La présente politique définit la manière dont l'organisation identifie, évalue et traite les vulnérabilités au sein de ses systèmes, applications et infrastructures.

1.2 Elle vise à réduire le risque de cybersécurité en imposant l'application des correctifs dans des délais appropriés ainsi que des pratiques de remédiation fondées sur les risques, adaptées aux petites et moyennes entreprises (PME).

1.3 La présente politique contribue à la conformité en vue de la certification ISO/IEC 27001:2022 et aide à satisfaire aux obligations réglementaires au titre du RGPD, de NIS2 et de DORA, en imposant une gestion proactive des vulnérabilités techniques.

1.4 L'organisation reconnaît que les systèmes non corrigés constituent une menace significative pour la sécurité de l'information et doivent être traités de manière systématique et sans délai.

2. Champ d’application

2.1 La présente politique s'applique à :

2.1.1 Tous les serveurs, postes de travail fixes, ordinateurs portables, appareils mobiles, équipements réseau et plateformes hébergées dans le cloud utilisés par l'organisation

2.1.2 Tous les systèmes d'exploitation, logiciels tiers, modules d'extension et applications utilisés dans le cadre des activités de l'organisation

2.1.3 Tous les membres du personnel informatique interne ou les prestataires externes responsables de la maintenance, des mises à jour ou de la surveillance des systèmes

2.1.4 Tout code développé sur mesure ou tout logiciel embarqué maintenu par l'organisation ou pour son compte

2.2 La présente politique couvre à la fois les infrastructures gérées directement par l'organisation et les systèmes administrés par des fournisseurs sous contrat ou des prestataires d'hébergement.

3. Objectifs

3.1 Identifier et évaluer les vulnérabilités connues sur l'ensemble des actifs informatiques en temps utile et de manière cohérente

3.2 Appliquer les correctifs et les mises à jour logicielles en fonction de leur criticité et du risque pesant sur les opérations de l'organisation ou sur les données à caractère personnel

3.3 Prévenir l'exploitation de faiblesses techniques susceptibles d'entraîner une interruption de service, une violation de données ou une non-conformité réglementaire

3.4 Tenir des enregistrements exacts des correctifs appliqués, des éléments en suspens et des exceptions, afin de permettre la préparation des audits

3.5 Utiliser des outils et des processus adaptés à la taille et à la complexité opérationnelle de l'organisation, sans compromettre leur efficacité

3.6 Soutenir la conformité légale et réglementaire, y compris l'article 32 du RGPD et l'Annexe A, mesure 8, de l'ISO/IEC 27001

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Assume la responsabilité globale de la mise en œuvre des activités de gestion des correctifs et des vulnérabilités

4.1.2 Approuve les exceptions au regard du risque lorsque les correctifs ne peuvent pas être appliqués et examine les stratégies d'atténuation associées

4.1.3 Examine les rapports sur l'état d'application des correctifs et veille à la disponibilité des ressources nécessaires pour respecter les exigences en matière de correctifs

4.2 Prestataire de support informatique / Administrateur informatique interne

4.2.1 Surveille les systèmes afin de détecter les vulnérabilités et les correctifs disponibles à l'aide des alertes fournisseurs, des avis de menace et des notifications du système d'exploitation

4.2.2 Applique les mises à jour du système d'exploitation, du micrologiciel et des applications dans les délais définis

4.2.3 Tient un journal formalisé des correctifs et documente les mises à jour non résolues ou reportées

4.2.4 Réalise les tests et la planification des mises à jour critiques afin de réduire au minimum les perturbations opérationnelles

[... 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 être revue au moins une fois par an par le directeur général, avec la contribution du prestataire informatique et du coordinateur à la protection des données

9.2 Déclencheurs de revue

9.2.1 Des revues intermédiaires doivent être réalisées si :

9.2.1.1 Une vulnérabilité majeure ou un code d'exploitation affecte des systèmes relevant du champ d'application

9.2.1.2 Des changements significatifs affectent les systèmes ou les logiciels

9.2.1.3 Un audit identifie des lacunes dans les processus de gestion des correctifs

9.2.1.4 Un incident ou une violation lié(e) à l'application des correctifs est enregistré(e)

9.3 Gestion des versions de la politique

9.3.1 Toutes les mises à jour doivent être consignées dans un journal des versions avec un résumé des modifications

9.3.2 Les modifications doivent être communiquées au personnel concerné

9.3.3 Les versions obsolètes doivent être archivées avec un accès restreint

10. Politiques associées et articulations

10.1 La présente politique soutient plusieurs autres politiques PME et s'articule avec elles :

10.1.1 P12S – Politique de gestion des actifs : identifie la propriété et la classification des systèmes afin de garantir que tous les actifs nécessitant l'application de correctifs sont recensés et inventoriés

10.1.2 P14S – Politique de conservation et d'élimination des données : garantit que les systèmes planifiés pour la mise hors service sont mis à jour de manière sécurisée ou effacés afin de réduire l'exposition aux vulnérabilités

10.1.3 P17S – Politique de protection des données et de la vie privée : priorise la remédiation des vulnérabilités pour les systèmes traitant des données à caractère personnel afin de respecter les obligations en matière de protection des données

10.1.4 P22S – Politique de journalisation et de surveillance : contribue à la détection des systèmes non corrigés ou des comportements suspects pouvant signaler l'exploitation d'une vulnérabilité

10.1.5 P30S – Politique de réponse aux incidents : définit les procédures de réponse aux vulnérabilités qui entraînent des incidents de sécurité, y compris les étapes d'escalade et de signalement

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Exige la mise en œuvre de contrôles permettant de traiter le risque opérationnel, y compris la gestion des vulnérabilités

11.2 ISO/IEC 27002

11.2.1 Mesure 8.8 – Précise les processus de détection et de correction des vulnérabilités connues dans les systèmes

11.2.2 Mesure 8.9 – Met l'accent sur la configuration sécurisée, la validation des correctifs et le contrôle des changements afin d'éviter de nouvelles expositions lors des mises à jour

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – Exige l'identification des vulnérabilités et leur remédiation dans des délais définis

11.3.2 SI-2 – Impose l'application rapide des correctifs et des mises à jour en fonction de leur criticité

11.3.3 CM-2 – Encadre les configurations de référence des systèmes et la documentation des mises à jour afin d'assurer une protection cohérente

11.4 RGPD (UE)

11.4.1 Article 32(1)(b) – Exige que les organisations mettent en œuvre des mesures techniques appropriées, y compris l'application des correctifs, afin de maintenir la sécurité du traitement

11.5 Directive NIS2 (UE)

11.5.1 Article 21(2)(d) – Exige le traitement des vulnérabilités au moyen d'une détection systématique et d'une remédiation

11.5.2 Article 21(2)(e) – Implique une configuration sécurisée et la gestion des correctifs afin d'assurer la résilience des TIC

11.6 DORA (UE)

11.6.1 Article 8(1) – Exige la détection et l'atténuation des risques liés aux TIC, y compris les vulnérabilités techniques

11.6.2 Article 10(2) – Impose aux entités financières de remédier aux faiblesses affectant les systèmes et opérations TIC

11.7 COBIT 2019

11.7.1 DSS05.02 – Exige le traitement des risques liés aux vulnérabilités techniques connues afin de maintenir des opérations sécurisées

11.7.2 APO12.01 – Aligne la gestion des risques sur une surveillance proactive et la correction des faiblesses des systèmes