					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P19					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	Traitement systématique des vulnérabilités techniques ; maintien dans la durée de l'efficacité des contrôles de sécurité.
ISO/IEC 27002:2022	Mesures 8.8, 8.9, 5	Lignes directrices de mise en œuvre relatives à l'application des correctifs, aux scans de vulnérabilités, à l'intégrité logicielle, à la configuration sécurisée et aux inventaires d'actifs.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Exige des scans fréquents, la remédiation des défauts et la gestion des configurations.
RGPD de l'UE	Article 32, Considérant 49	Mesures techniques visant l'application rapide des correctifs, le traitement des vulnérabilités et le maintien de la sécurité dans la durée.
Directive NIS2 de l'UE	Article 21(2)(d)	Détection, réponse et atténuation des vulnérabilités afin de maintenir un niveau élevé d'hygiène cyber.
Règlement DORA de l'UE	Articles 8, 10(2)(f)	Remédiation en temps utile des vulnérabilités liées aux TIC ; évaluations continues fondées sur les menaces.
COBIT 2019	DSS05.02, DSS01.03, MEA	Scanner, suivre et atténuer les faiblesses techniques ; surveiller les signes d'exploitation ; auditer l'efficacité, y compris l'état d'application des correctifs.

1. Objet

1.1 La présente politique définit les exigences obligatoires de l'organisation en matière d'identification, de classification, de remédiation et de surveillance des vulnérabilités techniques et des défauts logiciels sur l'ensemble des systèmes d'information et des actifs entrant dans le périmètre du SMSI.

1.2 Elle impose que toutes les vulnérabilités connues soient évaluées et traitées en temps utile selon une approche fondée sur les risques, au moyen d'une application coordonnée des correctifs, d'ajustements de configuration ou de contrôles compensatoires, en cohérence avec les besoins métier et les obligations de conformité.

1.3 Cette politique contribue à la conformité avec l'ISO/IEC 27001, annexe A, mesure 8.8, ainsi qu'avec les recommandations de l'ISO/IEC 27002, et répond aux exigences réglementaires prévues par l'article 8 de DORA, l'article 21 de NIS2, l'article 32 du RGPD et les domaines DSS et APO de COBIT 2019.

2. Champ d’application

2.1 La présente politique s’applique à tous les systèmes d’information, actifs et environnements qui stockent, traitent ou transmettent des données relevant de la gouvernance du SMSI, y compris :

2.1.1 les systèmes d’exploitation, applications, équipements réseau, micrologiciels, plateformes cloud, interfaces de programmation applicative (API) et logiciels tiers ;

2.1.2 les systèmes en développement, en préproduction, en production, de sauvegarde et de reprise après sinistre ;

2.1.3 les postes de travail, serveurs, équipements IoT, infrastructures de virtualisation et conteneurs.

2.2 Elle s’impose à :

2.2.1 l’ensemble du personnel interne : administrateurs informatiques, ingénieurs systèmes, développeurs d’applications, analystes sécurité et équipes d’infrastructure ;

2.2.2 les parties externes : sous-traitants, prestataires de services managés (MSP), éditeurs de logiciels et intégrateurs de systèmes assumant des responsabilités techniques sur les actifs concernés.

2.3 La politique couvre l’intégralité du cycle de vie des vulnérabilités et des correctifs, y compris :

2.3.1 les scans et la détection ;

2.3.2 la classification des risques et la priorisation ;

2.3.3 l’acquisition des correctifs, les tests, le déploiement et le retour arrière ;

2.3.4 la gestion des exceptions et la planification des contrôles compensatoires ;

2.3.5 la journalisation, l’établissement de rapports et la traçabilité à des fins d’audit.

3. Objectifs

3.1 Veiller à ce que toutes les vulnérabilités connues soient identifiées, évaluées et remédiées de manière à réduire au minimum l’exposition résiduelle et à respecter les priorités opérationnelles.

3.2 Établir des processus homogènes à l’échelle de l’organisation pour les scans de vulnérabilités, la classification de la sévérité (par exemple CVSS) et la gestion des correctifs, y compris le traitement d’urgence et la planification du retour arrière.

3.3 Permettre une gestion sécurisée des configurations, en l’alignant sur les configurations de référence de durcissement, les pratiques de gestion des changements et le renseignement sur les menaces en temps réel.

3.4 Assurer une conformité mesurable aux contrôles réglementaires et normatifs relatifs à l’intégrité des systèmes, à l’hygiène des correctifs et à la remédiation rapide des défauts.

3.5 Définir clairement les responsabilités et l’obligation de rendre compte entre les rôles pour l’ensemble du cycle de vie de gestion des vulnérabilités, afin que toutes les parties prenantes agissent dans les délais définis par les SLA et rendent compte des indicateurs de contrôle devant faire l’objet d’une notification.

3.6 Renforcer la préparation à l’audit et améliorer la résilience face aux menaces émergentes, y compris les vulnérabilités zero-day, les chaînes actives d’exploitation de code et les divulgations majeures des fournisseurs.

4. Rôles et responsabilités

4.1 Responsable de la sécurité des systèmes d’information (RSSI)

4.1.1 Est propriétaire de la politique et veille à son intégration dans le SMSI.

4.1.2 Définit l’appétence au risque de l’organisation et veille à son alignement avec les exigences réglementaires et de contrôle.

4.2 Responsable de la gestion des vulnérabilités / Responsable des opérations de sécurité

4.2.1 Supervise de bout en bout les opérations de gestion des vulnérabilités et des correctifs.

4.2.2 Coordonne les calendriers de scan, les modèles de priorisation et les échéances de remédiation.

4.2.3 Tient le registre des vulnérabilités et contribue à l’évaluation des contrôles compensatoires.

[... 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 ou lors de la survenance de l’un des événements suivants :

9.1.1 mises à jour réglementaires significatives (par exemple modifications de DORA ou de NIS2) ;

9.1.2 évolutions des référentiels de priorisation des vulnérabilités (par exemple mises à jour du CVSS) ;

9.1.3 changements majeurs de l’environnement informatique (par exemple migration vers le cloud, refonte de l’EDR) ;

9.1.4 violations majeures ou avis externes imposant un renforcement de la politique.

9.2 Les revues doivent être conduites par le RSSI en collaboration avec les opérations de sécurité, la gestion des risques et la direction de l’infrastructure.

9.3 Les mises à jour de la politique doivent être :

9.3.1 documentées dans le registre de contrôle documentaire du SMSI ;

9.3.2 revues et approuvées par la direction générale ;

9.3.3 communiquées à toutes les parties prenantes concernées, y compris aux sous-traitants traitant des données.

9.4 Les versions historiques doivent être conservées de manière sécurisée à des fins d’audit et de traçabilité.

10. Politiques associées et articulations

10.1 P1 - Politique de sécurité de l’information. Établit l’engagement général visant à protéger les systèmes et les données, y compris la gestion proactive des vulnérabilités et la préservation de l’intégrité logicielle.

10.2 P5 - Politique de gestion des changements. Encadre l’ensemble des déploiements de correctifs et des ajustements de configuration, en imposant la documentation, les tests, l’approbation et les procédures de retour arrière qui complètent les processus de remédiation des vulnérabilités.

10.3 P6 - Politique de gestion des risques. Soutient la classification et le traitement des vulnérabilités non remédiées au moyen d’évaluations structurées des risques, d’analyses d’impact et de procédures d’acceptation du risque résiduel.

10.4 P12 - Politique de gestion des actifs. Garantit que les systèmes sont inventoriés et classifiés avec exactitude, afin de permettre des scans de vulnérabilités cohérents, l’attribution des responsabilités et une couverture des correctifs sur l’ensemble du cycle de vie.

10.5 P22 - Politique de journalisation et de surveillance. Définit les exigences relatives à la détection des événements et à la constitution d’une piste d’audit. La présente politique contribue à la visibilité sur les activités d’application des correctifs, les changements non autorisés et les tentatives d’exploitation visant des vulnérabilités connues.

10.6 P30 - Politique de réponse aux incidents. Précise les protocoles d'escalade et les stratégies de confinement applicables aux vulnérabilités exploitées, aux investigations sur les violations et aux actions correctives alignées sur les contrôles de la présente politique.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001:2022 : clause 8.1 - Planification et maîtrise opérationnelles : impose un traitement systématique des vulnérabilités techniques afin de maintenir dans la durée l'efficacité des contrôles de sécurité.

11.2 ISO/IEC 27002:2022 - Mesures 8.8, 8.9, 5 : fournit des lignes directrices de mise en œuvre relatives à l'application des correctifs, aux scans de vulnérabilités, à l'intégrité logicielle, ainsi qu'à l'intégration avec la configuration sécurisée et les inventaires d'actifs.

11.3 NIST SP 800-53 Rev.5 : RA-5 - Surveillance et scan des vulnérabilités : exige des scans fréquents et le suivi de la remédiation. SI-2 - Remédiation des défauts : exige l'évaluation rapide et l'atténuation des défauts au moyen de correctifs disponibles ou d'autres mesures. CM-2 / CM-6 - Configurations de référence et contrôles de gestion des configurations : établit le socle des configurations sécurisées des systèmes liées à l'application des correctifs.

11.4 RGPD de l'UE (2016/679) : article 32 - Sécurité du traitement : impose la mise en œuvre de mesures techniques appropriées, telles que l'application rapide des correctifs et le traitement des vulnérabilités, afin d'assurer la confidentialité et la résilience des systèmes. Considérant 49 : encourage les entités à mettre en œuvre des contrôles préventifs contre les menaces connues afin de soutenir la sécurité et la continuité.

11.5 Directive NIS2 de l'UE (2022/2555) : article 21(2)(d) : impose aux entités essentielles et importantes de détecter, traiter et atténuer les vulnérabilités des systèmes et de maintenir un niveau élevé d'hygiène cyber.

11.6 Règlement DORA de l'UE (2022/2554) : article 8 - Gestion des risques liés aux TIC : impose l'identification et la remédiation en temps utile des vulnérabilités affectant les technologies de l'information et de la communication utilisées dans les systèmes financiers. Article 10(2)(f) : souligne l'importance d'évaluations continues des vulnérabilités fondées sur les menaces et de l'application des correctifs dans le cadre de la résilience opérationnelle.

11.7 COBIT 2019 : DSS05.02 - Gérer les vulnérabilités de sécurité : oriente les organisations vers le scan, le suivi et l'atténuation des faiblesses techniques connues. DSS01.03 - Surveiller l'infrastructure : garantit que les systèmes sont surveillés afin de détecter les signes d'exploitation ou de faiblesse. MEA03 - Surveiller, évaluer et apprécier la conformité : impose des audits réguliers de l'efficacité des contrôles, y compris de l'état d'application des correctifs et de la gestion des exceptions.