					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P39					Titre du document : **Politique de divulgation coordonnée des vulnérabilités**							
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	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
RGPD de l'UE	Art. 32(1)(d)	
NIS2 de l'UE	Art. 21(2)(e)	
DORA de l'UE	Art. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Objet

1.1 Établir un processus formel de réception, de traitement et de divulgation des informations relatives aux vulnérabilités affectant les systèmes ou services de l'organisation, conformément à l'article 21(2)(e) de NIS2 relatif au traitement et à la divulgation des vulnérabilités.

1.2 Encourager les chercheurs en sécurité externes, les partenaires et les utilisateurs à signaler les vulnérabilités de manière responsable (Coordinated Vulnerability Disclosure - CVD), et définir les modalités selon lesquelles l'organisation communique les informations relatives aux vulnérabilités aux parties prenantes.

2. Champ d’application

2.1 La présente politique s'applique à l'ensemble des systèmes de réseau et d'information détenus ou exploités par l'organisation, ainsi qu'à toute vulnérabilité identifiée dans ces systèmes.

2.2 Elle couvre les équipes internes (sécurité, informatique, développement) ainsi que toute partie externe signalant des vulnérabilités (par exemple, chercheurs, clients, fournisseurs). Elle régit également les communications avec les éditeurs de produits ou les prestataires de services lorsque leurs composants sont concernés par la vulnérabilité.

3. Objectifs

3.1 Détecter et corriger les vulnérabilités de sécurité dans des délais appropriés en s'appuyant à la fois sur les évaluations internes et sur les signalements externes.

3.2 Fournir des lignes directrices claires permettant aux déclarants externes de transmettre les informations sur les vulnérabilités de manière sûre et licite, et à l'organisation d'y répondre et d'y remédier efficacement.

3.3 Garantir l'alignement sur les exigences de NIS2 et sur les bonnes pratiques du secteur (ISO/IEC 29147 et ISO/IEC 30111) en matière de divulgation coordonnée des vulnérabilités, afin d'améliorer la sécurité globale de l'écosystème.

4. Rôles et responsabilités

4.1 Équipe de traitement des vulnérabilités (VRT) : équipe désignée, placée sous la responsabilité du RSSI ou du responsable de la gestion des vulnérabilités, chargée de recevoir et de trier les signalements de vulnérabilités, d'évaluer le risque et l'impact, et de coordonner la remédiation ainsi que la divulgation publique.

4.2 Équipes informatiques et de développement : elles travaillent avec la VRT pour valider les vulnérabilités signalées, développer et tester les correctifs ou mesures d'atténuation, puis déployer les corrections. Elles fournissent, si nécessaire, les détails techniques destinés aux avis de sécurité.

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Surveillance et audit

9.1 La VRT tient un registre de divulgation des vulnérabilités assurant le suivi de chaque signalement depuis sa réception jusqu'à sa clôture. Ce registre fait l'objet d'une revue mensuelle afin de garantir le traitement dans les délais des éléments ouverts. Les éléments en retard font l'objet d'une escalade.

9.2 L'audit interne ou un évaluateur de sécurité indépendant réalise chaque année une revue de l'efficacité du processus de traitement des vulnérabilités, par exemple en vérifiant qu'un échantillon de cas a été traité conformément à la politique, notamment en matière d'accusé de réception, de correction et de divulgation dans les délais. La revue vérifie également que le canal public de divulgation est opérationnel, par exemple que les courriels de test sont bien reçus et traités.

9.3 Les indicateurs relatifs aux vulnérabilités, notamment le volume par gravité et les délais de remédiation, sont consolidés trimestriellement et présentés au comité de gouvernance cybersécurité afin d'alimenter les mises à jour de l'évaluation des risques.

10. Revue et maintenance

10.1 La présente politique fait l'objet d'une revue au moins annuelle. En outre, toute évolution significative de notre environnement informatique, par exemple le lancement d'un nouveau service exposé à Internet, ou toute évolution réglementaire pertinente, par exemple de nouvelles exigences de l'Union européenne en matière de divulgation des vulnérabilités des produits, déclenche une revue exceptionnelle.

10.2 Les mises à jour de la politique intègrent les retours des déclarants externes et les enseignements issus des analyses internes post-incident. Les changements majeurs sont approuvés par le RSSI, communiqués à l'ensemble du personnel et publiés dans notre référentiel en ligne des politiques de sécurité à des fins de transparence.

11. Politiques associées et articulations

11.1 P01 – Politique de sécurité de l'information. Elle fixe le cadre de gestion et de divulgation des vulnérabilités.

11.2 P19 – Politique de gestion des vulnérabilités et des correctifs. Elle définit le dispositif interne de remédiation articulé avec la réception des signalements CVD.

11.3 P24 – Politique de développement sécurisé. Elle alimente les corrections et le durcissement du cycle de développement sécurisé à partir des problèmes signalés.

11.4 P25 – Politique relative aux exigences de sécurité des applications. Elle garantit que les produits intègrent des exigences de sécurité compatibles avec la divulgation.

11.5 P30 – Politique de réponse aux incidents. Elle traite l'exploitation active des vulnérabilités divulguées.

11.6 P31 – Politique de collecte des éléments de preuve et d'investigation forensique. Elle préserve les livrables justificatifs liés aux failles signalées ou exploitées.

11.7 P26 – Politique de sécurité des tiers et des fournisseurs. Elle coordonne les divulgations impliquant des composants fournis par des fournisseurs.

11.8 P37 – Politique de conformité juridique et réglementaire. Elle encadre les notifications, la rédaction de la clause de protection et la publication.

12. Références

12.1 Directive NIS2 (UE 2022/2555), article 21(2), point (e) (sécurité du développement et traitement/divulgation des vulnérabilités)

12.2 Règlement d'exécution (UE) 2024/2690 de la Commission, annexe, section 6.10 (exigences techniques relatives aux processus de traitement et de divulgation des vulnérabilités)

12.3 Guide technique de l'ENISA sur les mesures de gestion des risques de cybersécurité – section relative au traitement et à la divulgation des vulnérabilités

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (mesure A.5.7 relative au renseignement sur les menaces et à la divulgation des vulnérabilités ; mesure A.8.28 relative au développement sécurisé)

12.5 ISO/IEC 29147:2018 (lignes directrices pour la divulgation des vulnérabilités) et ISO/IEC 30111:2019 (lignes directrices pour les processus de traitement des vulnérabilités)