					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P24S					Titre du document : **Politique de développement sécurisé**							
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	Contrôles de sécurité pertinents pour les pratiques opérationnelles, y compris le développement sécurisé
ISO/IEC 27002:2022	Contrôles 8.25 à 8.27	Couvre le cycle de vie du développement sécurisé, les tests et les responsabilités de sécurité des développeurs tiers
NIST SP 800-53 Rev.5	SA-3 à SA-15, SI-10	Traite du cycle de vie du développement sécurisé, du contrôle d'accès et du traitement des vulnérabilités dans le développement
RGPD de l'UE	Article 25	Exige la protection des données dès la conception et par défaut dans le développement logiciel
NIS2 de l'UE	Article 21(2)(a), (e), (h)	Implique des politiques de développement sécurisé, la supervision de l'utilisation de l'open source et la documentation des mesures d'atténuation
DORA de l'UE	Articles 6(7), 9(1)(c), 10(2)(c)	Exigences de sécurité du cycle de vie pour les systèmes TIC critiques dans le secteur financier
COBIT 2019	BAI	Référentiel pour une gestion structurée, traçable et résiliente du développement sécurisé

1. Objet

1.1 La présente politique impose que l'ensemble des logiciels, scripts et outils web créés ou modifiés par l'organisation ou par ses partenaires externes soient développés de manière sécurisée, afin de réduire au minimum le risque de vulnérabilités, d'accès non autorisé aux données ou de perturbation des opérations.

1.2 Elle définit les règles obligatoires de développement sécurisé et les pratiques de codage sécurisé que tous les développeurs internes, prestataires et fournisseurs doivent respecter, indépendamment de la taille ou de la complexité du projet.

1.3 La présente politique vise à protéger les données clients, à prévenir les violations de données et à garantir que les logiciels créés ou personnalisés par ou pour l'organisation satisfassent aux audits de sécurité, aux exigences légales (par exemple, RGPD, NIS2, DORA) et aux exigences de certification ISO/IEC 27001.

2. Champ d'application

2.1 La présente politique s'applique à toute personne et à toute entité participant, pour le compte de l'organisation, au développement, à la personnalisation, au déploiement ou à l'administration des éléments suivants :

2.1.1 Sites web, applications ou outils d’automatisation

2.1.2 Scripts ou logiciels développés en interne

2.1.3 Code produit par des développeurs tiers ou des travailleurs indépendants

2.1.4 Modules d’extension, bibliothèques et composants logiciels intégrés dans les systèmes de production

2.2 Elle couvre tous les environnements utilisés pour les activités de développement, y compris :

2.2.1 Environnements de développement et de test

2.2.2 Environnements de préproduction

2.2.3 Systèmes de production utilisés pour exécuter du code développé sur mesure

2.3 La politique encadre également le traitement des données lors du développement et du déploiement, en particulier toute utilisation de données de production dans des systèmes hors production.

3. Objectifs

3.1 Prévenir l’introduction de défauts de sécurité ou de vulnérabilités dans les logiciels développés sur mesure ou par des tiers.

3.2 Garantir l’intégration des pratiques de codage sécurisé et de prévention des vulnérabilités à chaque phase du cycle de vie du développement logiciel.

3.3 Réduire les risques liés à l’utilisation de composants open source ou tiers en imposant une évaluation préalable appropriée et leur suivi.

3.4 Exiger une revue de code formelle et des tests de sécurité des applications avant toute mise en production.

3.5 Encadrer les accès aux environnements de développement et garantir leur séparation d’avec les systèmes de production.

3.6 Satisfaire aux exigences obligatoires des normes et réglementations internationales (par exemple, ISO/IEC 27001, RGPD, DORA, NIS2).

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Approuve la présente politique et en assume la responsabilité.

4.1.2 S’assure que toutes les activités de développement logiciel, qu’elles soient internes ou externalisées, sont conformes à la présente politique.

4.1.3 Examine et signe les contrats de développement ou de services comportant des clauses relatives au développement sécurisé.

4.1.4 Vérifie la conformité des fournisseurs au moyen de points de contrôle réguliers ou en demandant des éléments de preuve en matière de sécurité.

4.2 Développeur interne ou propriétaire d’application

4.2.1 Respecte les pratiques de codage sécurisé et de déploiement sécurisé.

4.2.2 Applique la liste de contrôle de développement sécurisé à chaque projet.

4.2.3 Valide la sécurité de tout composant open source ou tiers utilisé.

4.2.4 Signale immédiatement au DG toute vulnérabilité découverte.

[... 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 être revue par le Directeur général au moins une fois par an afin de :

9.1.1 Vérifier le maintien de la conformité avec ISO/IEC 27001, le RGPD, NIS2 et DORA

9.1.2 Prendre en compte l'évolution des menaces ou les changements des bonnes pratiques de développement sécurisé

9.1.3 Garantir la compatibilité avec tout nouvel outil, toute nouvelle plateforme ou toute nouvelle relation fournisseur

9.2 Des revues intermédiaires doivent être déclenchées par :

9.2.1 Tout incident de sécurité logicielle signalé

9.2.2 L'introduction d'un nouveau framework de développement ou d'une nouvelle plateforme d'hébergement

9.2.3 Un changement de partenaires tiers de développement

9.2.4 Des évolutions réglementaires ayant une incidence sur les logiciels ou les obligations de sécurité

9.3 Toutes les modifications apportées à la présente politique doivent être :

9.3.1 Documentées avec la date, un résumé du changement et l'approbation du DG

9.3.2 Communiquées clairement à l'ensemble du personnel interne et externe intervenant dans le développement

9.3.3 Conservées dans le cadre de la gestion des versions et de l'historique des modifications des politiques de l'organisation

9.4 Les versions mises à jour doivent être facilement accessibles, au moyen de plateformes internes, d'une documentation imprimée ou de services cloud accessibles aux fournisseurs.

10. Politiques associées et articulations

10.1 La présente politique soutient la mise en œuvre effective de plusieurs autres politiques de la PME et s'articule avec elles :

10.1.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : établit les responsabilités relatives à l'attribution et à la vérification des contrôles de sécurité du développement dans l'ensemble des projets et chez les fournisseurs.

10.1.2 P4S – Politique de contrôle d'accès : définit les règles de base pour limiter l'accès aux environnements de développement et aux référentiels de code, y compris la séparation des tâches.

10.1.3 P8S – Politique de sensibilisation et de formation à la sécurité de l'information : garantit que les développeurs internes et les prestataires comprennent les pratiques de codage sécurisé et les responsabilités de sécurité associées.

10.1.4 P17S – Politique de protection des données et de la vie privée : précise la manière dont les données à caractère personnel doivent être traitées lors des processus de développement, de test et de journalisation afin de respecter le RGPD.

10.1.5 P30S – Politique de réponse aux incidents : définit la manière dont les incidents de sécurité liés au développement doivent être signalés, évalués et traités, y compris les expositions liées au code.

10.2 L'ensemble de ces politiques fonctionne de manière complémentaire afin de rendre le développement sécurisé réalisable et vérifiable, y compris dans une organisation de petite taille ou disposant de ressources techniques limitées.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Exige la mise en œuvre de contrôles opérationnels, y compris en matière de développement sécurisé, alignés sur les objectifs métier et le niveau de risque.

11.2 ISO/IEC 27002

11.2.1 Mesure 8.25 – Recommande d'intégrer la sécurité tout au long du cycle de vie logiciel, y compris le contrôle du code source, la gestion des versions et les accès des développeurs.

11.2.2 Mesure 8.26 – Précise les méthodes de test des applications et de vérification des fonctionnalités de sécurité avant la mise en production.

11.2.3 Mesure 8.27 – Exige que les développeurs tiers respectent les mêmes normes de développement et que leurs responsabilités en matière de sécurité soient clairement définies.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 à SA-15 – Définissent les processus de développement sécurisé, y compris le contrôle d'accès des développeurs, les tests, la modélisation des menaces et la documentation.

11.3.2 SI-10 – Exige que les développeurs identifient et atténuent les faiblesses logicielles courantes et utilisent des outils automatisés lorsque cela est applicable.

11.4 RGPD de l'UE (2016/679)

11.4.1 Article 25 – La « protection des données dès la conception et par défaut » impose l'intégration de mesures de sécurité et de protection de la vie privée pendant la conception et le développement des logiciels, en particulier lorsque des données à caractère personnel sont traitées.

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

11.5.1 Article 21(2)(a), (e) et (h) – Exige des politiques de développement sécurisé, la supervision de l'utilisation de l'open source et la documentation des mesures d'atténuation des risques liés aux applications au sein des entités essentielles et importantes.

11.6 DORA de l'UE (2022/2554)

11.6.1 Articles 6(7), 9(1)(c) et 10(2)(c) – Imposent des obligations de sécurité du cycle de vie de développement aux entités du secteur financier, y compris aux PME, en particulier pour les systèmes TIC critiques.

11.7 COBIT 2019

11.7.1 BAI03 – « Gérer l'identification et la construction des solutions » soutient la mise en œuvre de contrôles de développement structurés mettant l'accent sur la sécurité, la traçabilité et la résilience, adaptés aux contraintes des PME.