					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P24					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**

1. Objet

1.1 La présente politique définit les exigences de sécurité obligatoires applicables aux activités de développement de logiciels et de systèmes au sein de l'organisation, y compris les projets internes, le développement externalisé et l'intégration de code tiers.

1.2 Elle a pour objectif de garantir que la sécurité est intégrée tout au long du cycle de vie du développement logiciel (SDLC) et que les vulnérabilités sont identifiées, atténuées et prévenues avant le déploiement en production.

1.3 La présente politique soutient la mise en œuvre de la clause 8.1 de l'ISO/IEC 27001:2022 et des contrôles 8.25 à 8.28 de l'annexe A, en normalisant la gouvernance du développement sécurisé, les pratiques de validation du code et la supervision du développement par des tiers.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble des éléments suivants :

2.1.1 Les logiciels, applications, scripts, intégrations et outils d'automatisation développés en interne ou par des tiers

2.1.2 Les équipes de développement, les responsables produit, les équipes DevOps, l'assurance qualité (QA), les architectes, les chefs de projet et les prestataires

2.1.3 Les environnements du cycle de vie du développement logiciel (SDLC), y compris les systèmes de développement, de test, de préproduction et de production

2.1.4 Les composants open source et tiers intégrés dans les applications internes

2.1.5 Les logiciels déployés sur site, dans des environnements de cloud privé, hybride ou public

2.2 Tous les utilisateurs et toutes les entités participant au développement, aux tests ou au déploiement de systèmes dans le contexte de l'organisation sont soumis à la présente politique, y compris les prestataires de services managés (MSP) et les fournisseurs de plateformes.

3. Objectifs

3.1 Intégrer des contrôles de sécurité à toutes les phases du développement logiciel, de la conception au déploiement, afin que la réduction des risques soit proactive et continue.

3.2 Prévenir l'introduction de vulnérabilités exploitables telles que les défauts d'injection, une authentification non sécurisée et l'exposition à des faiblesses connues de composants tiers.

3.3 Établir et mettre en œuvre des pratiques de programmation sécurisée alignées sur OWASP, SANS CWE et les lignes directrices propres aux cadres technologiques utilisés.

3.4 Garantir que tout code fait l'objet d'une revue par les pairs, d'analyses automatisées et d'une validation de sécurité avant déploiement.

3.5 Gérer les risques de développement découlant d'activités externalisées, de l'inclusion de code tiers et de la réutilisation de logiciels open source.

3.6 Protéger les environnements de développement, de test et de préproduction contre tout accès non autorisé et interdire l'utilisation de données de production sans masquage ou anonymisation approuvés.

3.7 Promouvoir la sensibilisation à la sécurité auprès des développeurs, des responsables produit et des professionnels de l'assurance qualité au moyen de formations adaptées aux rôles et de mises à jour continues sur les menaces émergentes.

4. Rôles et responsabilités

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

4.1.1 Est responsable de la présente politique et veille à l'application des exigences de développement sécurisé à l'échelle de l'organisation.

4.1.2 Approuve les normes de programmation sécurisée et les accords de développement avec des tiers.

4.1.3 Valide les décisions de traitement des risques relatives aux vulnérabilités non résolues ou reportées.

4.2 Responsable de la sécurité applicative / responsable DevSecOps

4.2.1 Élabore, maintient et promeut les lignes directrices de programmation sécurisée.

4.2.2 Intègre les tests de sécurité statiques et dynamiques dans les pipelines CI/CD.

4.2.3 Réalise des revues de sécurité du code et définit les actions de remédiation obligatoires.

[... 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 annuellement, ou plus fréquemment en réponse à :

9.1.1 Des révisions majeures des méthodologies de développement ou de l’outillage DevOps

9.1.2 Des incidents de sécurité significatifs résultant de vulnérabilités applicatives

9.1.3 Des évolutions des exigences réglementaires liées à la sécurité des logiciels (par exemple RGPD, DORA)

9.1.4 De nouvelles normes sectorielles ou de nouveaux renseignements sur les menaces (par exemple OWASP Top 10, SLSA, MITRE CWE)

9.2 La revue de la politique doit être conduite par le responsable de la sécurité applicative, en coordination avec le RSSI, les architectes logiciels, les responsables QA et le service juridique (pour les implications liées au code tiers).

9.3 Toute révision doit être consignée dans le registre de contrôle documentaire du SMSI, faire l’objet d’une gestion de versions et être communiquée aux équipes concernées au moyen de notes de version ou d’une formation obligatoire.

9.4 Les versions antérieures doivent être conservées dans le référentiel d’archives à des fins de traçabilité juridique et d’audit.

10. Politiques associées et articulations

10.1 P1 – Politique de sécurité de l’information. Définit l’orientation stratégique imposant l’intégration de la sécurité dans l’ensemble des systèmes d’information, dont le développement sécurisé constitue un contrôle opérationnel fondamental.

10.2 P4 – Politique de contrôle d’accès. Définit les mesures de contrôle applicables à la restriction des accès aux environnements de développement, référentiels, outils de build et pipelines CI/CD.

10.3 P5 – Politique de gestion des changements. Garantit que les changements de code, les mises en production et les déploiements sont soumis à une approbation appropriée, à des plans de retour arrière et à une vérification après déploiement.

10.4 P12 – Politique de gestion des actifs. Soutient l’inventaire des environnements de développement, des référentiels source et des systèmes de build en tant qu’actifs gérés soumis à classification et protection.

10.5 P22 – Politique de journalisation et de surveillance. S’applique aux pipelines de développement afin de garantir que les processus de build, les promotions de code et les événements de déploiement sont journalisés, surveillés et analysés pour détecter les anomalies de sécurité.

10.6 P30 – Politique de réponse aux incidents. Fournit le cadre d’analyse et de réponse aux défauts de sécurité découverts après déploiement ou lors des tests de sécurité applicative.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001:2022

11.1.1 Clause 8.1 – Planification et maîtrise opérationnelles : impose l'intégration des processus et contrôles de développement sécurisé dans les opérations.

11.2 ISO/IEC 27002:2022 – Contrôles 8.25 à 8.28

11.2.1 Annexe A Contrôle 8.25 – Cycle de vie de développement sécurisé : impose l'intégration formelle de la sécurité dans la conception et le développement des logiciels.

11.2.2 Annexe A Contrôle 8.26 – Exigences de sécurité applicative : exige la définition de règles de programmation sécurisée et de critères d'acceptation de sécurité.

11.2.3 Annexe A Contrôle 8.27 – Architecture système sécurisée et principes d'ingénierie : impose l'application de principes de conception de sécurité et l'atténuation des faiblesses connues.

11.2.4 Annexe A Contrôle 8.28 – Codage sécurisé : exige l'application de pratiques de codage sécurisé tout au long du développement.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-3 à SA-15 : établit des pratiques structurées de développement de la sécurité des applications, y compris des exigences relatives à la conception, à l'intégrité du code et aux tests.

11.3.2 SI-10 – Validation des entrées d'information : traite des défenses liées à la programmation sécurisée.

11.3.3 SR-3 – Sécurité de la chaîne d'approvisionnement : exige l'évaluation des logiciels tiers, des composants et des prestataires de développement.

11.4 RGPD de l'UE (2016/679)

11.4.1 Article 25 – Protection des données dès la conception et par défaut : impose l'intégration de la sécurité et de la protection de la vie privée dans le développement des systèmes.

11.4.2 Article 32 – Sécurité du traitement : soutient des mesures techniques telles que la validation des entrées, les contrôles d'accès et le déploiement sécurisé.

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

11.5.1 Article 21(2)(e–f) : exige des pratiques de développement logiciel intégrant la gestion des vulnérabilités, la sécurité du code et le signalement des incidents.

11.6 DORA de l'UE (2022/2554)

11.6.1 Article 9 – Gestion des risques liés aux TIC : impose des pratiques de développement sécurisé pour les entités financières, y compris des contrôles de qualité logicielle et la remédiation des défauts.

11.6.2 Article 10 – Continuité d'activité et tests : encourage des tests rigoureux et la validation des systèmes TIC, y compris les applications.

11.7 COBIT 2019

11.7.1 BAI03 – Gérer l'identification et la construction des solutions : encadre la conception, le développement et l'intégration de la sécurité dans les nouvelles solutions.

11.7.2 BAI07 – Gérer l'acceptation du changement et la transition : garantit un déploiement sécurisé et une évaluation après déploiement.

11.7.3 DSS05 – Gestion des services de sécurité : applique la validation de sécurité aux logiciels et au provisionnement des services.