Politique de Gestion du Développement Sécurisé

1. Objectif

E1: Assurer que toutes les applications et systèmes développés respectent les principes de sécurité dès leur conception afin de réduire les risques de vulnérabilités.

2. Champ d'application

E2: Cette politique s'applique à l'ensemble des équipes de développement, DevOps, et aux prestataires impliqués dans la conception, le développement et la maintenance des logiciels de l'entreprise.

3. Principes du Développement Sécurisé

E3: Intégration des pratiques de sécurité dès les premières phases du développement (Security by Design).
E4: Adoption du modèle OWASP pour l'identification et la mitigation des vulnérabilités courantes.
E5: Mise en œuvre de contrôles d'accès stricts pour le code source et les environnements de développement.
E6: Chiffrement des données sensibles en transit et au repos.
E7: Automatisation des tests de sécurité (SAST, DAST) à chaque étape du cycle de développement.

4. Exigences en Matière de Sécurité

E8: Utilisation de frameworks et bibliothèques sécurisés et maintenus à jour.
E9: Mise en place de revues de code systématiques avec un focus sur la sécurité.
E10: Gestion rigoureuse des secrets et clés d'API (stockage sécurisé, rotation régulière).
E11: Sensibilisation continue des équipes de développement aux menaces cyber et aux bonnes pratiques de sécurité.

5. Gestion des Incidents et Conformité

E12: Plan de réponse aux incidents de sécurité applicative.
E13: Suivi et correction rapide des vulnérabilités identifiées.
E14: Respect des normes et réglementations en vigueur (ISO 27001, RGPD, NIS2, etc.).

6. Surveillance et Amélioration Continue

E15: Réalisation d'audits de sécurité réguliers sur le code et les applications.
E16: Tests de pénétration périodiques pour identifier et corriger les failles de sécurité.
E17: Mise à jour continue des pratiques de développement sécurisé en fonction des nouvelles menaces et technologies.

Cette politique est révisée au moins une fois par an ou après la découverte d’une vulnérabilité critique.