					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P28					Titre du document : **Politique de développement externalisé**							
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 8.1	N/A
ISO/IEC 27002:2022	Mesures 5.19-5.22, 8	N/A
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-10	N/A
RGPD de l'UE	Articles 28, 32	N/A
NIS2 de l'UE	Articles 21(2)(a), (h), 23	N/A
DORA de l'UE	Articles 28(1), (2)	N/A
COBIT 2019	APO10, BAI03, DSS	N/A

1. Objet

1.1 La présente politique définit les contrôles obligatoires applicables à l'externalisation du développement de logiciels ou de systèmes auprès de fournisseurs externes, de sous-traitants ou d'agences, afin de garantir l'intégration de pratiques sécurisées tout au long du cycle de vie du développement.

1.2 Elle vise à prévenir les vulnérabilités de sécurité, les pertes de données, l'exposition de la propriété intellectuelle (PI) et les manquements de conformité résultant de prestations de développement externalisées.

1.3 La politique impose des exigences en matière de gouvernance des fournisseurs, de développement sécurisé, de gestion des accès, de supervision et de réversibilité en fin de contrat afin de préserver la confidentialité, l'intégrité et la disponibilité des logiciels développés.

2. Champ d'application

2.1 La présente politique s'applique à toutes les unités organisationnelles qui ont recours à des entités externes pour le développement de logiciels ou de systèmes, y compris :

2.1.1 les applications web, les applications mobiles, les systèmes embarqués, les interfaces de programmation d'applications (API), les scripts, les flux d'approbation automatisés ou les modules de plateforme ;

2.1.2 les développements sur mesure pour des plateformes internes, des systèmes destinés aux clients ou des produits commerciaux ;

2.1.3 les prestations confiées à des développeurs tiers, des travailleurs indépendants, des agences ou des équipes offshore.

2.2 La politique s'applique également à toute entité externe accédant au code source, aux environnements de test ou aux pipelines CI/CD pendant le développement.

2.3 Les exigences s'appliquent quel que soit le type de contrat, la méthodologie de développement ou la localisation géographique du prestataire externalisé.

3. Objectifs

3.1 Imposer des pratiques de cycle de vie de développement sécurisé (SDLC) pour l'ensemble des prestations externalisées, de la planification à la validation post-déploiement.

3.2 Garantir que tous les contrats conclus avec des développeurs externes incluent des clauses obligatoires relatives à la protection des données, au développement sécurisé et à la conservation de la propriété intellectuelle.

3.3 Définir les exigences de contrôle d'accès, de supervision et d'audit applicables aux développeurs tiers interagissant avec les systèmes internes.

3.4 Protéger l'organisation contre les risques liés à la chaîne d'approvisionnement, les manquements juridiques et les atteintes à la réputation associés aux logiciels développés en externe.

3.5 Maintenir une conformité continue avec les référentiels de sécurité, notamment ISO/IEC 27001, NIST, le RGPD, NIS2, DORA et COBIT 2019.

4. Rôles et responsabilités

4.1 Haute direction

4.1.1 Approuve les projets de développement externalisé à haut risque et valide les dérogations à la politique lorsqu'elles sont justifiées.

4.1.2 Veille à ce que les décisions d'externalisation soient alignées sur les objectifs stratégiques et l'appétence au risque de l'organisation.

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

4.2.1 Approuve l'intégration des fournisseurs du point de vue de la sécurité.

4.2.2 Définit les exigences de contrôle de sécurité applicables aux prestations externalisées et examine les rapports d'incident.

[... 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 une fois par an, ou plus fréquemment dans les circonstances suivantes :

9.1.1 l'introduction de nouveaux modèles d'externalisation du développement, de nouveaux fournisseurs ou de nouvelles juridictions ;

9.1.2 des mises à jour des cadres réglementaires tels que le RGPD, NIS2 ou DORA ;

9.1.3 à la suite d'un incident de sécurité impliquant du code externalisé, des accès ou des livrables ;

9.1.4 dans le cadre de constats d'audit interne ou d'améliorations du SMSI.

9.2 Le responsable de la sécurité des systèmes d'information (RSSI) est chargé d'initier et de coordonner la revue de la politique en consultation avec :

9.2.1.1 le Juridique et les Achats (pour l'alignement contractuel) ;

9.2.1.2 les chefs de projet et responsables produit (pour la faisabilité opérationnelle) ;

9.2.1.3 la Sécurité de l'information (pour les mises à jour relatives aux menaces et aux contrôles) ;

9.2.1.4 la haute direction (pour l'approbation finale).

9.3 Toute mise à jour de la politique doit :

9.3.1.1 être soumise à une gestion de versions et stockée dans un référentiel documentaire désigné ;

9.3.1.2 être communiquée aux parties prenantes impliquées dans les activités de développement externalisé ;

9.3.1.3 être articulée avec toute mise à jour des politiques associées ou de la documentation procédurale.

9.4 Un journal des modifications doit accompagner chaque version de la politique afin d'assurer la traçabilité des modifications et des approbations.

10. Politiques associées et articulations

10.1 La présente politique soutient les documents associés suivants et s'articule avec eux :

10.1.1 P1 - Politique de sécurité de l'information : établit les principes de sécurité à l'échelle de l'entreprise applicables aux contextes de développement interne et de développement par des tiers.

10.1.2 P5 - Politique de gestion des changements : garantit que tous les changements liés au déploiement provenant de bases de code externalisées sont revus et approuvés avant mise en œuvre.

10.1.3 P13 - Politique de classification et d'étiquetage des données : détermine comment les données sensibles sont identifiées avant leur exposition à des fournisseurs de développement ou à des dépôts de code.

10.1.4 P18 - Politique relative aux contrôles cryptographiques : encadre la manière dont les clés, secrets et identifiants sensibles doivent être traités pendant le développement et la livraison.

10.1.5 P24 - Politique de développement sécurisé : définit les exigences minimales applicables aux pratiques de développement logiciel internes et externes.

10.1.6 P30 - Politique de réponse aux incidents : régit la manière dont les violations ou problèmes de sécurité liés au développement externalisé sont remontés, investigués et résolus.

10.1.7 P33 - Politique d'audit et de surveillance de la conformité : définit les exigences de revue des activités de développement externalisé dans le cadre des audits ou des revues de conformité.

11. Normes et référentiels de référence

11.1 La présente politique s'aligne sur des référentiels et réglementations de sécurité reconnus au niveau international afin d'assurer l'externalisation sécurisée du développement logiciel et l'encadrement des fournisseurs.

11.2 ISO/IEC 27001

11.2.1 Clause 8.1 - Planification et maîtrise opérationnelles : impose des contrôles de processus pour le développement sécurisé et les prestations de tiers.

11.3 ISO/IEC 27002:2022 - Mesures 5.19 à 5.21, 8

11.3.1 Annexe A, mesure 5.19 - Gestion des relations avec les fournisseurs : exige des accords formels comportant des clauses de sécurité et de conformité.

11.3.2 Annexe A, mesure 5.20 - Prise en compte de la sécurité de l'information dans les accords fournisseurs : garantit que les contrôles spécifiques au développement sont intégrés dans les contrats.

11.3.3 Annexe A, mesure 5.21 - Gestion de la fourniture de services par les fournisseurs : implique la surveillance des livrables et des risques liés au développement tiers.

11.3.4 Annexe A, mesure 8.27 - Développement externalisé : impose des exigences de sécurité définies et des contrôles d'accès applicables aux logiciels développés en externe.

11.3.5 Ces mesures définissent des exigences structurées pour la sélection, la contractualisation et la supervision des développeurs externalisés, y compris les pratiques de développement sécurisé, le traitement du code et la validation des performances.

11.4 NIST SP 800-53 Rev.5

11.4.1 SA-4 - Processus d'acquisition : exige que les exigences de développement sécurisé soient définies au moment de l'acquisition.

11.4.2 SA-9 - Services de systèmes externes : encadre la manière dont les développeurs tiers interagissent de manière sécurisée avec les services internes.

11.4.3 SA-10 - Gestion de la configuration des développeurs : s'aligne sur les obligations de gestion de versions, d'accès au code et de suivi des changements pour les équipes externes.

11.5 RGPD de l'UE (2016/679)

11.5.1 Article 28 - Obligations du sous-traitant : exige que les contrats conclus avec des développeurs tiers précisent les exigences de sécurité, de contrôle et d'audit applicables au traitement de données à caractère personnel.

11.5.2 Article 32 - Sécurité du traitement : impose des mesures de protection appropriées (par exemple chiffrement, contrôle d'accès) lors du développement de systèmes traitant des données à caractère personnel.

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

11.6.1 Articles 21(2)(a), (h), 23 : imposent l'application de pratiques de développement sécurisé dans les relations avec les tiers et au sein des chaînes d'approvisionnement numériques, avec supervision et vérification technique.

11.7 DORA de l'UE (2022/2554)

11.7.1 Articles 28(1), (2) : imposent aux entités financières de gérer le risque lié aux TIC associé aux tiers au moyen de contrôles contractuels et d'une supervision sécurisée du développement, en particulier pour les développements externalisés critiques.

11.8 COBIT 2019

11.8.1 APO10 - Gérer les fournisseurs : établit des exigences structurées relatives à l'évaluation des fournisseurs, aux contrats et à la surveillance des performances.

11.8.2 BAI03 - Gérer la conception et la construction des solutions : correspond directement aux processus SDLC sécurisés, aux revues de code et à la validation du développement.

11.8.3 DSS05 - Gestion des services de sécurité : s'aligne sur la surveillance et la protection des systèmes développés en externe ou par des tiers.