					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P28S					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 la réglementation

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	Clauses 5.1, 6.1, 8	Contrôles applicables du SMSI et contrôles relatifs aux fournisseurs
ISO/IEC 27002:2022	Contrôles 5.19, 5.20, 8.25–8.27	Contrôles relatifs aux fournisseurs et au cycle de vie du développement sécurisé
NIST SP 800-53 Rév. 5	SA-4, SA-9, SA-11, SA-15, SR-3	Exigences relatives à l'acquisition, à la chaîne d'approvisionnement, au développement sécurisé et aux accords conclus avec les fournisseurs
RGPD de l'UE	Article 28	Exigences contractuelles et de protection des données applicables au traitement effectué par des tiers
NIS2 de l'UE	Article 21(2)(a), (h)	Contrôles relatifs à la chaîne d'approvisionnement et au développement sécurisé des applications
DORA de l'UE	Article 10	Gestion des risques liés aux tiers relevant des TIC, y compris le développement externalisé
COBIT 2019	BAI03, DSS05	Exigences applicables au développement externe et aux prestataires de services informatiques

1. Objet

1.1 La présente politique garantit que tout développement logiciel externalisé, qu'il soit confié à des freelances, à des agences ou à des prestataires tiers, est réalisé de manière sécurisée, encadré contractuellement et conforme aux exigences légales, réglementaires et d'audit applicables.

1.2 Elle protège l'organisation contre les risques liés à un code non sécurisé, à une propriété insuffisamment définie, à l'exposition des données et à une gestion inadéquate des fournisseurs, en imposant des normes de développement opposables et une supervision des prestataires, y compris en l'absence de service informatique dédié.

1.3 La présente politique contribue à la certification ISO/IEC 27001:2022 en définissant clairement les attentes en matière de développement, les responsabilités et les contrôles documentés applicables aux activités de développement réalisées par des tiers.

2. Champ d'application

2.1 La présente politique s'applique à :

2.1.1 Tous les développeurs externalisés, y compris les freelances et les agences de développement

2.1.2 Tout travail de développement portant sur des outils internes, des sites web publics, des applications logicielles ou des automatisations métier

2.1.3 Le personnel chargé de sélectionner, gérer ou superviser des développeurs externes

2.1.4 Toute intégration de systèmes tiers, tout script ou tout développement interagissant avec les données ou les systèmes de l'entreprise

2.2 Elle couvre également tout tiers ou toute plateforme disposant d'un accès aux identifiants de l'entreprise, aux référentiels de données, aux dépôts de code source, aux environnements de préproduction ou aux systèmes de production.

3. Objectifs

3.1 Garantir que tout développement externalisé respecte les principes de développement sécurisé et que les développeurs sont contractuellement tenus de respecter des normes documentées et des clauses de confidentialité.

3.2 Établir la propriété de l'ensemble des livrables — code, actifs, identifiants et documentation — en garantissant le transfert complet des droits à l'entreprise et une remise traçable à l'achèvement du projet.

3.3 Prévenir les risques courants de développement, notamment la réutilisation de code propriétaire, les attaques de la chaîne d'approvisionnement via des bibliothèques, l'utilisation de frameworks non maintenus et l'octroi d'un accès administrateur non validé.

3.4 Exiger une documentation préalable à l'engagement pour chaque projet externalisé, y compris les contrats, les accords de non-divulgation et les exigences minimales de sécurité.

3.5 Protéger les données clients, les systèmes et les processus internes en imposant une supervision renforcée du développement, des tests après livraison et une gestion sécurisée des accès aux systèmes.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Approuve toutes les relations avec les fournisseurs et signe les accords de développement.

4.1.2 Veille à ce que tout développement externalisé respecte la présente politique.

4.1.3 Supprime les accès aux systèmes de l'entreprise à l'issue du projet.

4.1.4 Examine la documentation et les résultats post-livraison.

4.2 Responsable de projet (généralement un employé interne ou un coordinateur désigné)

4.2.1 Assure la coordination quotidienne avec le développeur externe.

4.2.2 Vérifie que les exigences fonctionnelles sont satisfaites et que les livrables sont testés.

4.2.3 Veille à la remise sécurisée du code et des identifiants.

4.2.4 Signale au DG tout problème ou incident lié au développement.

[... 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 Revue annuelle

9.1.1 La présente politique doit être revue par le Directeur général (DG) au moins une fois par an. Cette revue vérifie qu'elle continue de répondre :

9.1.1.1 Aux exigences de certification ISO/IEC 27001

9.1.1.2 Aux évolutions des obligations légales (par exemple, article 28 du RGPD, article 10 de DORA)

9.1.1.3 Aux pratiques actuelles de développement propres aux PME et aux risques liés aux tiers

9.2 Revues intermédiaires

9.2.1 Des revues de la politique doivent également avoir lieu lorsque :

9.2.1.1 Un nouveau fournisseur ou une nouvelle plateforme de développement externalisé est intégré

9.2.1.2 Un incident significatif impliquant un développement externalisé se produit

9.2.1.3 Des modifications substantielles interviennent dans les outils, plateformes ou environnements utilisés

9.3 Processus de revue

9.3.1 Le DG est responsable de :

9.3.1.1 Vérifier que les contrats, accords de non-divulgation et processus de contrôle d'accès demeurent efficaces

9.3.1.2 Confirmer que les fournisseurs et freelances actuels sont alignés sur la politique

9.3.1.3 Réviser les dispositions sur la base des retours issus des projets ou incidents passés

9.4 Gestion des versions et communication

9.4.1 Toutes les modifications doivent être :

9.4.1.1 Enregistrées avec la date, le motif et la description du changement

9.4.1.2 Approuvées par le DG et ajoutées à l'historique des versions

9.4.1.3 Communiquées à l'ensemble du personnel ou aux responsables de projet travaillant avec des développeurs externes

9.4.1.4 Redistribuées à tous les fournisseurs et tiers concernés lorsque nécessaire

10. Politiques associées et articulations

10.1 La présente politique soutient directement la mise en œuvre des politiques suivantes, alignées sur le contexte PME, et s'y articule :

10.1.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : précise les responsabilités en matière d'approbation des fournisseurs, de contrôle d'accès et d'acceptation du risque lors du recours à des développeurs externalisés.

10.1.2 P4S – Politique de contrôle d'accès : définit les règles de création, de restriction et de suppression des comptes utilisateurs et des accès administrateur utilisés dans le cadre du développement externalisé.

10.1.3 P8S – Politique de sensibilisation et de formation à la sécurité de l'information : garantit que le personnel interne comprend comment coordonner de manière sécurisée le travail avec des développeurs externes, notamment pour la gestion des identifiants et des fichiers de projet.

10.1.4 P17S – Politique de protection des données et de la vie privée : établit les exigences de sécurité et les exigences légales applicables au traitement des données à caractère personnel susceptibles d'être traitées par des développeurs externalisés au titre du RGPD.

10.1.5 P24S – Politique de développement sécurisé : précise comment le développement interne et externe doit respecter les pratiques de développement sécurisé ainsi que la validation des bibliothèques et frameworks.

10.1.6 P30S – Politique de réponse aux incidents : requise lorsqu'un développement externalisé entraîne des incidents de sécurité ou des vulnérabilités, afin d'orienter l'investigation coordonnée et la remédiation.

10.2 Ces politiques doivent être mises en œuvre en parallèle afin de garantir que le développement externalisé ne crée pas de risque non maîtrisé et n'entraîne pas de manquement aux obligations de conformité de la PME.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 6.1 – Les organisations doivent évaluer et traiter les risques de sécurité de l'information associés aux fournisseurs.

11.1.2 Clause 8.1 – Exige une planification et une maîtrise opérationnelles, y compris pour les services tiers tels que le développement externalisé.

11.2 ISO/IEC 27002

11.2.1 Contrôle 5.19 – Recommande d'évaluer la capacité des fournisseurs à satisfaire aux exigences de sécurité de l'information.

11.2.2 Contrôle 5.20 – Recommande une surveillance régulière et une revue périodique des services tiers.

11.2.3 Contrôles 8.25–8.27 – Définissent les pratiques du cycle de vie du développement sécurisé applicables au développement externalisé.

11.3 NIST SP 800-53 Rév.

11.3.1 SA-4 – Exige que les stratégies d'acquisition intègrent des mesures de sécurité de l'information.

11.3.2 SA-9 – Traite du développement de systèmes externes et des risques liés à la chaîne d'approvisionnement.

11.3.3 SA-11 – Définit des pratiques de développement sécurisé, y compris la revue de code et la remédiation des défauts.

11.3.4 SA-15 – Encourage l'usage d'outils automatisés pour la détection des défauts et l'assurance logicielle.

11.3.5 SR-3 – Exige que les accords avec les fournisseurs incluent des exigences de cybersécurité.

11.4 Règlement général sur la protection des données de l'UE (RGPD)

11.4.1 Article 28 – Exige que les contrats conclus avec des sous-traitants tiers garantissent des mesures de protection des données appropriées, exigence directement applicable aux développeurs qui traitent des données à caractère personnel ou y accèdent.

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

11.5.1 Article 21(2)(a), (h) – Exige des contrôles de sécurité de la chaîne d'approvisionnement et des pratiques de développement logiciel sécurisé pour les prestataires de services numériques relevant de son champ d'application, y compris les PME lorsque cela est applicable.

11.6 Règlement européen sur la résilience opérationnelle numérique (DORA)

11.6.1 Article 10 – Exige une gestion des risques liés aux tiers relevant des TIC, y compris les accords de développement, les obligations de sécurité et les contrôles des risques associés aux prestataires tiers.

11.7 COBIT 2019

11.7.1 BAI03 – Gérer l'identification et la construction des solutions – garantit que le développement externe répond aux exigences métier et aux attentes de sécurité.

11.7.2 DSS05 – Gérer les services de sécurité – exige que les services de sécurité externes et les prestataires de développement opèrent dans le respect de règles de sécurité appliquées et sous supervision.