					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P26S					Titre du document : **Politique de sécurité des tiers et des fournisseurs**							
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 opérationnels applicables aux relations avec les tiers et les fournisseurs
ISO/IEC 27002:2022	Mesures 5.19 à 5.22	Contrôles de sécurité des fournisseurs, clauses contractuelles de sécurité, gestion des changements, surveillance et revue
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Acquisition, configuration, accords d'interconnexion et contrôles applicables au personnel externe
RGPD de l'UE	Articles 28, 32	Accords de traitement des données, exigences de sécurité applicables aux sous-traitants
NIS2 de l'UE	Articles 21(2)(a)(b)(i), 23(1)	Gestion des risques liés à la chaîne d'approvisionnement, supervision des services fournis par des tiers
DORA de l'UE	Articles 5(1)(2), 28(1)(2)	Gestion des risques liés aux TIC pour les prestataires tiers
COBIT 2019	APO10, APO12, DSS05 Gestion des services de sécurité	Gestion des fournisseurs et intégration des risques

1. Objet

1.1 La présente politique définit les exigences de sécurité obligatoires applicables à l'engagement, à la gestion et à la cessation des relations avec les tiers et les fournisseurs qui accèdent aux données, aux systèmes ou aux services de l'organisation, ou qui ont une incidence sur ceux-ci.

1.2 Elle impose que les prestataires externes — y compris les prestataires de support informatique, les opérateurs de services cloud, les développeurs logiciels et les sous-traitants de processus métier — assurent un traitement sécurisé des actifs de l'entreprise, dans le respect des lois et normes applicables.

1.3 La présente politique vise à réduire les risques tels que les fuites de données, les modifications non autorisées des systèmes, les sanctions réglementaires ou les interruptions d'activité causées par des dispositifs tiers insuffisamment sécurisés ou mal gouvernés.

2. Champ d'application

2.1 La présente politique s'applique à tous les tiers qui :

2.1.1 fournissent des logiciels, des infrastructures, des services d'hébergement ou des services cloud

2.1.2 accèdent aux systèmes, équipements ou applications internes, ou les administrent

2.1.3 traitent des données, des documents ou des données de sauvegarde de l'entreprise

2.1.4 soutiennent les opérations métier, les ressources humaines, la finance ou les services clients

2.2 Elle s'applique également :

2.2.1 au personnel interne impliqué dans la sélection, le recrutement ou la supervision des fournisseurs

2.2.2 à tout personnel chargé de l'intégration des fournisseurs, des contrats, des accès ou des revues

2.2.3 à tout système ou processus dépendant de composants ou de services tiers

3. Objectifs

3.1 Veiller à ce que tous les fournisseurs respectent des exigences de sécurité clairement définies.

3.2 Exiger que les contrats fournisseurs incluent des obligations opposables en matière de sécurité, de protection de la vie privée et de réponse aux incidents.

3.3 Évaluer et documenter les risques liés aux fournisseurs avant la signature des accords ou l'octroi d'un accès.

3.4 Soumettre les fournisseurs critiques ou à haut risque à des revues régulières afin de confirmer leur conformité.

3.5 Établir un processus formel de gestion des dérogations, des incidents et des mises à jour contractuelles.

3.6 Soutenir la conformité aux obligations de gouvernance des fournisseurs prévues par l'ISO/IEC 27001:2022, le RGPD, NIS2 et DORA.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 assume la responsabilité finale de la sélection des fournisseurs et de la conformité en matière de sécurité

4.1.2 approuve les contrats, les dérogations et les escalades impliquant des fournisseurs

4.1.3 supervise la réponse aux incidents et la prise de décision lorsqu'un fournisseur ne respecte pas ses obligations

4.2 Prestataire de services informatiques externe ou référent interne sécurité/conformité

4.2.1 évalue les accès techniques demandés par les fournisseurs

4.2.2 met en œuvre les règles de contrôle d'accès, procède à la revue des journaux et vérifie le traitement sécurisé des données

4.2.3 examine les éléments de preuve relatifs aux contrôles de sécurité, aux certifications ou aux résultats d'audit, le cas échéant

[... 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 au moins une fois par an par le Directeur général, avec la participation du prestataire de services informatiques ou du responsable des fournisseurs.

9.2 La politique doit également être revue :

9.2.1 après tout changement significatif des obligations juridiques, réglementaires ou contractuelles

9.2.2 à la suite d'un incident de sécurité ou d'un constat d'audit lié à un fournisseur

9.2.3 lors de l'introduction de nouvelles catégories de fournisseurs (par exemple plateformes SaaS critiques)

9.3 Toute mise à jour doit être :

9.3.1 documentée avec l'historique des versions et sa justification

9.3.2 approuvée par le Directeur général

9.3.3 communiquée au personnel interne concerné et aux responsables des fournisseurs

9.3.4 conservée avec les versions précédentes conformément à la P14S – Politique de conservation et d'élimination des données

10. Politiques associées et articulations

10.1 L'efficacité de la présente politique dépend d'une coordination avec les politiques PME suivantes de sécurité de l'information :

10.1.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : attribue la responsabilité de la supervision des fournisseurs et de l'application des contrats.

10.1.2 P4S – Politique de contrôle d'accès : définit les règles de restriction d'accès à appliquer lorsqu'un fournisseur se voit accorder un accès à un système.

10.1.3 P17S – Politique de protection des données et de la vie privée : garantit que les fournisseurs traitant des données à caractère personnel respectent les principes de protection des données et les exigences légales.

10.1.4 P14S – Politique de conservation et d'élimination des données : s'applique à toute donnée ou à tout enregistrement partagé avec des fournisseurs ou stocké par eux et encadre l'élimination sécurisée après la résiliation du contrat.

10.1.5 P30S – Politique de réponse aux incidents : définit la réponse à apporter lorsqu'un fournisseur est à l'origine d'un incident de sécurité ou y est impliqué, y compris les procédures d'escalade et de collecte des éléments de preuve.

10.2 Ces politiques fonctionnent conjointement afin de garantir que le risque lié aux fournisseurs est maîtrisé tout au long du cycle de vie du contrat.

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 ceux appliqués aux relations avec les tiers et les fournisseurs.

11.2 ISO/IEC 27002

11.2.1 Mesure 5.19 – Veille à ce que les mesures de sécurité des fournisseurs soient alignées sur les exigences de l'organisation.

11.2.2 Mesure 5.20 – Exige des accords formels couvrant les dispositions de sécurité, les responsabilités et les obligations en cas de violation.

11.2.3 Mesure 5.21 – Encadre les changements dans les services fournisseurs susceptibles d'affecter le niveau de sécurité.

11.2.4 Mesure 5.22 – Exige la surveillance et la revue des services fournisseurs et de leur conformité.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Encadre l'acquisition de systèmes et de services externes en imposant des évaluations des risques et des attentes définies.

11.3.2 SA-10 – Encadre les procédures de configuration et de changement impliquant des systèmes administrés par des tiers.

11.3.3 CA-3 – Exige des accords d'interconnexion pour les systèmes impliquant des entités externes.

11.3.4 PS-7 – Définit les exigences de filtrage et de responsabilité applicables au personnel externe.

11.4 RGPD de l'UE (2016/679)

11.4.1 Article 28 – Exige des accords de traitement des données avec les fournisseurs agissant en qualité de sous-traitants.

11.4.2 Article 32 – Implique des mesures techniques et organisationnelles (MTO) appropriées pour tous les sous-traitants traitant des données.

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

11.5.1 Article 21(2)(a), (b), (i) – Implique la gestion des risques liés à la chaîne d'approvisionnement TIC et les contrôles applicables aux tiers.

11.5.2 Article 23(1) – Exige une supervision documentée des services tiers pour les entités essentielles et importantes.

11.6 DORA de l'UE (2022/2554)

11.6.1 Article 5(1) – Exige un cadre de gestion des risques liés aux TIC couvrant tous les prestataires tiers critiques.

11.6.2 Article 5(2) – Prévoit des contrôles contractuels et opérationnels pour les dépendances aux services TIC.

11.6.3 Article 28(1), (2) – Établit des règles de supervision du risque TIC lié aux tiers dans le secteur financier.

11.7 COBIT 2019

11.7.1 APO10 – « Gérer les fournisseurs » décrit les contrôles d'approvisionnement et les attentes en matière de gestion de la relation.

11.7.2 APO12 – « Gérer les risques » intègre le risque fournisseur dans la gouvernance des risques de l'organisation.

11.7.3 DSS05 Gestion des services de sécurité – s'applique aux fournisseurs de services managés et aux prestataires de services externalisés.