| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insérez ici la dénomination de l'entité juridique enregistrée | | | | | | | |
| Numéro du document :<br>P26 | | | | | Titre du document :<br>**Politique de sécurité des tiers et des fournisseurs** | | | | | | | |
| Version :<br>1.0 | | Date d'entrée en vigueur :<br>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 | Planification et maîtrise opérationnelles : exige des contrôles formels sur les services tiers ayant un impact sur le SMSI |
| ISO/IEC 27002:2022 | Mesures 5.19 à 5.22 | Politiques et procédures relatives aux relations avec les fournisseurs ; gestion des risques liés aux fournisseurs ; gestion de la prestation des services fournisseurs ; surveillance et revue des fournisseurs |
| NIST SP 800-53 Rev.5 | SA-9, SA-10, CA-3, PS-7 | Services de systèmes externes ; gestion des configurations de développement ; interconnexions des systèmes ; sécurité du personnel tiers |
| RGPD de l'UE | Articles 28, 32, 33 | Obligations des sous-traitants ; sécurité du traitement ; notification d'une violation de données à caractère personnel |
| NIS2 de l'UE | Article 21(2)(e–f) | Gestion des fournisseurs fondée sur les risques et supervision de la sécurité |
| DORA de l'UE | Articles 28, 30 | Risque lié aux tiers TIC ; supervision des prestataires tiers critiques de services TIC |
| COBIT 2019 | BAI05, DSS02, MEA03 | Gérer l'accompagnement du changement organisationnel ; gérer les demandes de service et les incidents ; surveiller, évaluer et apprécier la conformité |

**1. Objet**

1.1 La présente politique définit les exigences de sécurité de l'information applicables à l'établissement, à la gestion et au maintien de relations sécurisées avec les fournisseurs tiers et les prestataires de services.

1.2 Elle impose que tous les fournisseurs ayant accès aux données, aux systèmes ou à l'infrastructure de l'organisation soient soumis à des contrôles de sécurité rigoureux, à des garanties contractuelles et à une surveillance continue tout au long du cycle de vie du service.

1.3 La politique soutient les mesures de l'Annexe A 5.19 à 5.22 de l'ISO/IEC 27001 en intégrant les exigences de sécurité dans les processus d'approvisionnement, d'intégration, de diligence raisonnable des fournisseurs, de gestion contractuelle, de surveillance des services et de fin de relation.

**2. Champ d'application**

**2.1 La présente politique s'applique à :**

2.1.1 tous les fournisseurs tiers, sous-traitants, prestataires de services cloud et organismes de services qui traitent des actifs informationnels de l'organisation ou y accèdent ;

2.1.2 tous les rôles internes intervenant dans l'évaluation des fournisseurs, l'intégration, la contractualisation, la gestion des risques, la surveillance ou la fin de relation ;

2.1.3 toutes les relations fournisseurs comportant un accès à des données sensibles, une intégration avec des services de production ou un support à des fonctions métier critiques.

2.2 Elle couvre à la fois les fournisseurs directs et, le cas échéant, leurs sous-traitants ultérieurs, et inclut les logiciels tiers, l'infrastructure, le support et les services managés.

**3. Objectifs**

3.1 Veiller à ce que les risques de sécurité liés aux fournisseurs soient identifiés, évalués et atténués de manière cohérente tout au long du cycle de vie de la relation.

3.2 Intégrer des exigences de sécurité normalisées dans tous les contrats fournisseurs, y compris les obligations de notification de violation, les clauses de droit d'audit et les responsabilités en matière de protection des données.

3.3 Exiger des diligences préalables formelles relatives aux fournisseurs et des évaluations des risques documentées avant l'engagement de nouveaux fournisseurs ou le renouvellement d'accords de service à haut risque.

3.4 Établir des mécanismes de surveillance continue de la conformité des fournisseurs, y compris des évaluations de performance, des audits et l'escalade des incidents.

3.5 Encadrer les changements apportés aux services des fournisseurs et imposer une fin de relation sécurisée ainsi que la restitution ou la destruction des données à l'échéance du contrat.

3.6 Aligner les contrôles de sécurité des tiers sur les obligations réglementaires et contractuelles applicables, notamment le RGPD, NIS2, DORA et les normes ISO/IEC 27001.

**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 son alignement avec le SMSI global, la gestion des risques et la stratégie de conformité.

4.1.2 Approuve les niveaux de classification des fournisseurs, les résultats des revues de sécurité et les dérogations à haut risque.

4.1.3 Participe à l'escalade des incidents graves impliquant des fournisseurs ainsi qu'aux négociations contractuelles relatives aux services critiques.

**4.2 Achats et gestion des fournisseurs**

4.2.1 Veillent à ce que tous les contrats nouveaux ou renouvelés avec des fournisseurs intègrent des clauses approuvées en matière de sécurité et de protection des données.

4.2.2 Tiennent à jour le registre centralisé des fournisseurs et coordonnent avec les ressources humaines et le service juridique les éléments de documentation relatifs aux risques liés aux tiers.

4.2.3 Lancent les processus d'intégration et veillent à leur alignement avec les évaluations de sécurité précontractuelles.

[ ... 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 annuelle, ou plus tôt en cas de :**

9.1.1 changement significatif de la stratégie d'approvisionnement ou de l'écosystème fournisseurs ;

9.1.2 mise à jour des cadres juridiques ou réglementaires (par exemple : DORA, RGPD) ;

9.1.3 incident majeur impliquant un tiers, violation de données ou échec d'audit ;

9.1.4 constats issus d'évaluations des risques ou d'organismes externes de certification.

9.2 Le processus de revue relève conjointement du RSSI, des achats, du service juridique et des fonctions de gestion des risques.

9.3 Toutes les révisions de la politique doivent être documentées dans le registre de contrôle documentaire du SMSI, faire l'objet d'une gestion des versions et être communiquées aux parties prenantes concernées au moyen des instances de gouvernance fournisseurs et des programmes de sensibilisation.

9.4 Les versions remplacées doivent être archivées pendant une durée minimale de trois ans afin d'assurer la traçabilité et la conformité juridique.

**10. Politiques associées et articulations**

10.1 P1 – Politique de sécurité de l'information. Établit l'engagement global visant à sécuriser l'ensemble des opérations de l'organisation, y compris celles reposant sur des fournisseurs tiers et des prestataires externes de services.

10.2 P6 – Politique de gestion des risques. Encadre l'identification, l'évaluation et l'atténuation des risques associés aux relations avec des tiers, y compris les risques hérités ou systémiques provenant des écosystèmes fournisseurs.

10.3 P17 – Politique de protection des données et de la vie privée. S'applique à tous les fournisseurs qui traitent des données à caractère personnel et impose des dispositions contractuelles appropriées, des garanties de transfert et les principes de protection de la vie privée dès la conception.

10.4 P4 – Politique de contrôle d'accès. Encadre les modalités d'accès du personnel tiers aux systèmes de l'organisation en imposant des autorisations fondées sur les rôles, des contrôles de session et des procédures de révocation.

10.5 P22 – Politique de journalisation et de surveillance. Exige que l'accès des fournisseurs aux systèmes fasse l'objet d'une surveillance, d'une journalisation et d'une revue, en particulier dans les environnements où se déroulent des activités à privilèges ou centrées sur les données.

10.6 P30 – Politique de réponse aux incidents. Définit les procédures d'escalade et les exigences de signalement des violations pour les événements de sécurité provenant de fournisseurs ou pour les investigations conjointes impliquant des systèmes tiers.

**11. Normes et référentiels de référence**

11.1 ISO/IEC 27001 : clause 8.1 – Planification et maîtrise opérationnelles : exige des contrôles formels sur les services tiers ayant un impact sur le SMSI.

**11.2 ISO/IEC 27002:2022 – Mesures 5.19 à 5.22 :**

11.2.1 Mesure de l'Annexe A 5.19 – Politiques et procédures relatives aux relations avec les fournisseurs : impose des contrôles pour gérer les interactions avec les fournisseurs.

11.2.2 Mesure de l'Annexe A 5.20 – Gestion des risques liés aux fournisseurs : porte sur l'identification, l'évaluation et la supervision continue du niveau de sécurité des fournisseurs.

11.2.3 Mesure de l'Annexe A 5.21 – Gestion de la prestation des services fournisseurs : exige un alignement de la performance et de la sécurité sur les attentes contractuelles.

11.2.4 Mesure de l'Annexe A 5.22 – Surveillance et revue des fournisseurs : renforce la nécessité d'une validation continue et d'une réévaluation de la conformité des tiers.

**11.3 NIST SP 800-53 Rev.5 :**

11.3.1 SA-9 – Services de systèmes externes : définit les exigences de sécurité et de risque applicables aux systèmes exploités par des entités externes.

11.3.2 SA-10 – Gestion des configurations de développement : s'applique lorsque des tiers fournissent des logiciels ou des environnements.

11.3.3 CA-3 – Interconnexions des systèmes : exige une supervision et un accord sur les flux de données entre les systèmes des différentes entités.

11.3.4 PS-7 – Sécurité du personnel tiers : garantit que les prestataires et le personnel des fournisseurs font l'objet de vérifications et d'une surveillance appropriées.

**11.4 RGPD de l'UE (2016/679) :**

11.4.1 Article 28 – Obligations des sous-traitants : impose des accords écrits avec les sous-traitants du traitement de données, comprenant des mesures techniques et organisationnelles (MTO).

11.4.2 Article 32 – Sécurité du traitement : impose des garanties appropriées tant aux responsables du traitement qu'aux sous-traitants.

11.4.3 Article 33 – Notification d'une violation de données à caractère personnel : impose une notification rapide par les fournisseurs en cas de violation.

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

11.5.1 Article 21(2)(e–f) : exige une gestion des fournisseurs fondée sur les risques et une supervision de la sécurité, en particulier dans les chaînes d'approvisionnement numériques des entités essentielles et importantes.

**11.6 DORA de l'UE (2022/2554) :**

11.6.1 Article 28 – Risque lié aux tiers TIC : impose des obligations en matière d'évaluation des risques, de dispositions contractuelles de sécurité et de stratégies de sortie pour les prestataires de services financiers.

11.6.2 Article 30 – Supervision des prestataires tiers critiques de services TIC : établit des attentes renforcées en matière de surveillance et de supervision pour les fournisseurs clés.

**11.7 COBIT 2019 :**

11.7.1 BAI05 – Gérer l'accompagnement du changement organisationnel : veille à ce que les transitions fournisseurs soient gouvernées de manière sécurisée.

11.7.2 DSS02 – Gérer les demandes de service et les incidents : s'applique aux incidents signalés par les fournisseurs et à l'intégration de la gestion des incidents.

11.7.3 MEA03 – Surveiller, évaluer et apprécier la conformité : renforce la mesure de la performance des fournisseurs et la surveillance de la conformité.