[Logo de l'organisation]

[Nom de l'organisation]

Commented [AES1]: Remplissez tous les champs entre crochets [ ] dans ce document.

POLITIQUE DE SECURITE DES FOURNISSEURS

Commented [AES2]: Pour apprendre à sélectionner les clauses de sécurité, consultez ces articles :

- 6-step process for handling supplier security according to ISO 27001 https://advisera.com/27001academy/blog/2014/06/30/6-step-process-for-handling-supplier-security-according-to-iso-27001/
- Which security clauses to use for supplier agreements? https://advisera.com/27001academy/blog/2017/06/19/which-security-clauses-to-use-for-supplier-agreements/

Code :	
Version :	
Date de la version :	
Créé par :	
Approuvée par :	
Niveau de confidentialité :	

Commented [AES3]: Le système de codage des documents doit être aligné avec le système existant de l'organisation pour la codification des documents ; au cas où un tel système n'est pas en place, cette ligne peut être supprimée.

Historique des modifications

Date	Version	Créé par	Description de la modification
	0.1	Advisera	Structure documentaire de base

Table des matières

1. But, domaine d'application et utilisateurs

Ce document a pour but de définir les règles relatives aux relations avec les fournisseurs et les partenaires, y compris les fournisseurs de services Cloud.

Ce document s'applique à tous les fournisseurs et partenaires qui ont la faculté d'influer sur la confidentialité, l'intégrité et l'accessibilité des informations sensibles de [nom de l'organisation].

Les utilisateurs de ce document sont la direction et les personnes responsables des fournisseurs et des partenaires au sein de [nom de l'organisation].

Commented [AES4]: Cette politique de haut niveau est rédigée conformément à la mesure A.5.19 de l'Annexe A de la norme ISO 27001, définissant les exigences de réduction des risques associés à l'accès des fournisseurs aux actifs de l'organisation, mais n'indique aucune pratique précise à adopter.

Si votre organisation souhaite définir des pratiques précises, que les fournisseurs doivent adopter, consultez un modèle du document de Politique de sécurité des technologies de l'information dans le dossier "05_Politiques_generales" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES5]: Indiquez le nom de votre organisation.

Commented [AES6]: Indiquez le nom de votre organisation.

2. Documents référencés

- Norme ISO/IEC 27001, clauses A.5.7, A.5.11, A.5.19, A.5.20, A.5.21, A.5.22, A.5.23, A.6.1, A.6.2, A.6.3 et A.8.30
- Méthodologie d'évaluation et de traitement des risques
- Rapport d'évaluation et de traitement des risques
- Politique de contrôle d'accès
- Déclaration de confidentialité

Commented [AES7]: Vous pouvez consulter un modèle pour ce document dans le dossier "06_Evaluation_et_traitement_des_risques" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES8]: Vous pouvez consulter un modèle pour ce document dans le dossier "06_Evaluation_et_traitement_des_risques" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

3. Relations avec les fournisseurs et les partenaires

3.1. Identification des risques

Commented [AES9]: Supprimer cette section si la mesure [illegible]

Les risques de sécurité relatifs aux fournisseurs et aux partenaires, y compris les fournisseurs de services Cloud, sont identifiés au cours du processus d'évaluation des risques, conformément à la Méthodologie d'évaluation et de traitement des risques. Au cours de l'évaluation des risques, une attention particulière doit être portée à l'identification des risques relatifs aux technologies d'information et de communication, ainsi que des risques relatifs à la chaîne d'approvisionnement des produits.

[Titre du poste] décide, par ailleurs, de la nécessité d'évaluer les risques relatifs aux fournisseurs ou partenaires individuels.

3.2. Evaluation préalable

Commented [AES10]: Supprimer cette section si la mesure [illegible]

[Titre du poste] décide de la nécessité d'effectuer des vérifications des antécédents des fournisseurs et partenaires individuels et, si oui, des méthodes qui doivent être utilisées.

Commented [AES11]: Par ex. expérience avec leurs autres [illegible]

3.3. Contrats

Commented [AES12]: Supprimer cette section si la mesure [illegible]

[Titre du poste] est chargé de déterminer les clauses de sécurité à inclure dans le contrat avec un fournisseur ou un partenaire. [illegible]

Les clauses suivantes doivent figurer dans les accords avec les fournisseurs :

- Protéger la confidentialité des informations
- La restitution des actifs après la résiliation de l'accord
- [illegible]
- [illegible]

Une liste de clauses est proposée dans Clauses de sécurité relatives aux fournisseurs et aux partenaires.

[illegible]

[Titre du poste] détermine le propriétaire du contrat pour chaque contrat, c'est-à-dire la personne responsable d'un fournisseur ou d'un partenaire particulier.

3.4. Formation et sensibilisation

Le propriétaire du contrat détermine quels employés, des fournisseurs et des partenaires, doivent suivre un programme de formation et de sensibilisation à la sécurité.

[illegible]

3.5. Contrôle et examen

Le propriétaire du contrat doit régulièrement vérifier et contrôler le niveau de services et le respect des clauses de sécurité par les fournisseurs ou les partenaires, les rapports et les enregistrements créés par les fournisseurs / partenaires, ainsi qu'auditer le fournisseur ou le partenaire au moins une fois par an.

[illegible]

3.6. Modification ou résiliation des services d'un fournisseur

Le propriétaire du contrat propose la modification ou la résiliation du contrat, et [titre du poste] prend la décision finale. [illegible]

3.7. Suppression des droits d'accès / restitution des actifs

Lorsque le contrat est modifié ou résilié, les droits d'accès des employés des fournisseurs / partenaires doivent être supprimés, conformément à la Politiques de contrôle d'accès.

[illegible]

Commented [AES13]: Indiquez le nom de votre organisation.

Commented [AES14]: Supprimer cette section si la mesure [illegible]

Commented [AES15]: Vous pouvez suggérer cette formation au fournisseur, pour sensibiliser ses employés et évaluer leurs connaissances : [illegible]

Commented [AES16]: Supprimer cette section si la mesure [illegible]

Commented [AES17]: Si nécessaire il est possible d'élaborer [illegible]

Commented [AES18]: Des audits sur site doivent être réalisés, [illegible]

Commented [AES19]: Pour en savoir plus sur ce sujet, consultez cet article : [illegible]

Commented [AES20]: Adapter si nécessaire, c'est-à-dire [illegible]

Commented [AES21]: Il s'agit généralement du Responsable sécurité.

Commented [AES22]: Supprimer cette section si la mesure [illegible]

Commented [AES23]: Supprimer ce paragraphe si la mesure [illegible]

Commented [AES24]: Supprimer ce paragraphe si la mesure [illegible]

4. Gestion des enregistrements conservés sur la base de ce document

[illegible]	[illegible]	*Personne responsable de la conservation*	*Mesures pour la protection des enregistrements*	[illegible]
[illegible]	[illegible]	[titre du poste]	Seul [titre du poste] a accès à [armoire, coffre-fort].	[illegible]
[illegible]	[illegible]	Propriétaire du contrat	Seul le propriétaire du contrat peut accéder à ces enregistrements.	[illegible]

Commented [AES25]: Modifiez ces enregistrements pour les faire correspondre aux pratiques de votre organisation. [illegible]

Commented [AES26]: Adaptez la durée dans cette colonne à [illegible]

5. Validité et gestion documentaire

Ce document est valide à compter du [date].

[illegible]

Commented [AES27]: Il ne s'agit que d'une recommandation ; [illegible]

Lors de l'évaluation de l'efficacité et de la pertinence de ce document, les critères suivants doivent être considérés :

- le nombre et l'importance des incidents résultant d'activités des fournisseurs et des partenaires
- [illegible]

[titre du poste]
[nom]

[signature]

Commented [AES28]: Nécessaire uniquement si la Procédure pour le contrôle des documents et des enregistrements prescrit que les documents papier doivent être signés.