



Politique de gestion des tiers

Responsable de la politique : CEO

Date d'entrée en vigueur : 23 Février 2024

Visée

Assurer la protection des données et des actifs de l'entreprise transmis aux fournisseurs et accessibles ou gérés par ces derniers, y compris les parties externes ou les entreprises tierces telles que des prestataires de services, des partenaires et des clients, et maintenir un niveau convenu de sécurité de l'information et de prestation de services conformément aux contrats conclus avec les fournisseurs.

Le présent document décrit une liste de base de dispositifs de contrôle de sécurité dont Evalandgo Software exige le respect de la part de ses partenaires et d'autres sociétés tierces lorsque ceux-ci utilisent des données confidentielles de Evalandgo Software.

Champ d'application

Toutes les données et tous les systèmes d'information détenus ou utilisés par Evalandgo Software qui sont essentiels à ses activités et/ou utilisent, stockent ou transmettent des données confidentielles. La présente politique s'applique à tous les employés de Evalandgo Software ainsi qu'à toutes les parties externes, y compris, mais sans s'y limiter, les consultants, sous-traitants, partenaires commerciaux, prestataires, fournisseurs, partenaires, prestataires de services externalisés de Evalandgo Software et autres entités tierces ayant accès aux données, systèmes, réseaux ou ressources système de Evalandgo Software.

Politique

Les exigences en matière de sécurité de l'information visant à limiter les risques associés à l'accès des fournisseurs aux actifs de l'entreprise doivent être convenues avec le fournisseur et documentées.

Pour tous les fournisseurs de services qui peuvent accéder aux systèmes, réseaux ou données confidentielles de Evalandgo Software, une diligence raisonnable doit être effectuée avant d'accorder l'accès ou de mettre en service des activités de traitement. Les informations doivent être conservées en fonction des exigences réglementaires ou de certification qui sont gérées ou qui concernent chaque fournisseur de services, et qui sont gérées par Evalandgo Software selon les besoins. Les exigences réglementaires ou de certification applicables suivantes, ou d'autres cadres de référence, normes de conformité ou réglementations, peuvent être incluses : ISO 27001, SOC 2, PCI-DSS, CCPA et RGPD.

Sécurité de l'information dans les relations avec des tiers

Aborder la sécurité dans les contrats

Des exigences en matière de sécurité de l'information doivent être établies et convenues avec chaque fournisseur susceptible de traiter, de stocker, de transmettre, d'avoir un impact sur la

sécurité des données confidentielles et des systèmes ou d'y avoir accès, ou de fournir des composants d'infrastructure informatique physique ou virtuelle à Evalandgo Software.

Pour tous les fournisseurs de services qui peuvent accéder aux systèmes de production de Evalandgo Software, ou avoir une incidence sur la sécurité de l'environnement de production de Evalandgo Software, des contrats écrits doivent être maintenus et mentionner la reconnaissance par le fournisseur de services de ses responsabilités en matière de confidentialité des données de l'entreprise et des clients, ainsi que tout engagement par rapport aux dispositifs de contrôle d'intégrité, de disponibilité et/ou de confidentialité qu'ils gèrent afin de répondre aux normes et exigences que Evalandgo Software a établies conformément au programme de sécurité de l'information de Evalandgo Software ou à tout cadre de référence pertinent.

Chaîne logistique des technologies

Evalandgo Software examinera et évaluera les risques associés aux fournisseurs et à la chaîne logistique des technologies. Lorsque cela est justifié, les contrats avec les fournisseurs doivent inclure des exigences visant à traiter les risques de sécurité de l'information pertinents associés aux services des technologies de l'information et de la communication et à la chaîne logistique.

Gestion des prestations de services tiers

Surveillance et évaluation des services tiers

Evalandgo Software doit régulièrement surveiller et évaluer les prestations de services des fournisseurs. Le niveau de performance de la sécurité et de la prestation de services des fournisseurs doit être évalué au moins une fois par an.

Gestion des modifications apportées aux services tiers

Les modifications apportées aux prestations de services des fournisseurs, y compris les modifications apportées aux contrats, aux services, aux technologies, aux politiques, aux procédures ou aux contrôles, doivent être gérées en tenant compte du caractère critique des informations, systèmes et processus de l'entreprise concernés. Evalandgo Software évaluera le risque de toute modification importante apportée par les fournisseurs et effectuera les modifications appropriées aux contrats et aux services en conséquence.

Gestion des risques liés aux tiers

Evalandgo Software veillera à ce que les éventuels risques posés par le partage de données confidentielles ou la fourniture d'un accès aux systèmes de l'entreprise soient identifiés, documentés et traités conformément à la présente politique. La gestion des risques joue un rôle essentiel dans la gouvernance et la gestion de l'entreprise au niveau stratégique et opérationnel. L'objectif d'une politique de sécurité des partenaires et des tiers est de s'assurer que les partenariats et les services atteignent leurs objectifs opérationnels en cohérence avec les exigences de Evalandgo Software en matière de sécurité de l'information.

Evalandgo Software ne doit pas partager ou transmettre des données confidentielles à un tiers sans d'abord effectuer une évaluation des risques du tiers et avoir signé un contrat écrit, un cahier des charges ou un contrat de service qui décrit les niveaux de service attendus et toute exigence spécifique en matière de sécurité de l'information.

Sécurité de l'information pour l'utilisation des services cloud

Cette section décrit les paramètres fondamentaux pour gérer et atténuer les risques liés à l'utilisation des services cloud.

Responsabilités et gestion des risques :

- Les rôles et responsabilités liés à l'utilisation et à la gestion des services cloud se trouvent dans la *Politique relative aux rôles et aux responsabilités*.
- Les risques liés à la sécurité des informations associés à l'utilisation des services cloud doivent être gérés conformément à ladite politique et à la *Politique de gestion des risques*.

Exigences et contrôle de sécurité :

- L'entreprise est responsable de tous les contrôles effectués par le client, tels que définis dans les matrices de responsabilité des fournisseurs de services cloud.

Gestion des incidents :

- Incidents de sécurité des informations liés aux services cloud gérés conformément au Plan de réponse aux incidents.

Examen du service et stratégie de sortie :

- Les risques liés à la sortie et à la dépendance vis-à-vis d'un fournisseur doivent être évalués avant l'acquisition dans le cadre de l'évaluation de la sécurité du fournisseur.

Contrat entre le fournisseur et le client :

- Les contrats avec les fournisseurs de services cloud spécifieront les protections relatives à la disponibilité des données et des services pour Evalandgo Software, même si elles peuvent être prédéfinies et non négociables.
- Dans la mesure du possible, Evalandgo Software demandera une notification préalable aux fournisseurs concernant les modifications substantielles en termes de prestation de services, y compris les modifications au niveau de l'infrastructure technique, de la localisation du stockage des données ou du recours à des sous-traitants.

Gestion continue et garanties :

- Les informations concernant la manière d'obtenir et d'utiliser les capacités de sécurité de l'information fournies par le fournisseur de services cloud doivent être évaluées dans le cadre de l'examen du fournisseur au moment de l'acquisition.

Normes de sécurité des tiers

Tous les tiers doivent maintenir des contrôles organisationnels et techniques raisonnables comme Evalandgo Software l'estime nécessaire.

L'évaluation de tiers qui reçoivent, traitent ou stockent des données confidentielles ou accèdent aux ressources de Evalandgo Software doit couvrir les contrôles suivants, le cas échéant, en fonction du service fourni et du degré de sensibilité des données stockées, traitées ou échangées.

Politique de sécurité de l'information

Les tiers maintiennent des politiques de sécurité de l'information qui reçoivent le soutien de leur direction générale et sont régulièrement révisées.

Évaluation et traitement des risques

Les tiers maintiennent des programmes d'audit, d'évaluation et de gestion des risques liés à l'information et aux technologies.

Sécurité des opérations

Les tiers mettent en œuvre des pratiques et des procédures commercialement raisonnables conçues pour garantir la sécurité des opérations selon les besoins. Ces actions de protections peuvent inclure les éléments suivants :

- Tests techniques
- Protection contre les logiciels malveillants
- Protection et gestion des réseaux
- Gestion des vulnérabilités techniques
- Journalisation et surveillance
- Réponse aux incidents
- Calendrier de continuité des activités

Contrôle des accès

Les tiers assurent le maintien d'un programme de contrôle des accès techniques.

Développement sécurisé de systèmes

Les tiers assurent le maintien d'un programme de développement sécurisé conforme aux meilleures pratiques du secteur en matière de développement de logiciels et de systèmes, comprenant des évaluations des risques, une gestion formelle des modifications, des normes de codage, une révision du code ainsi que des tests.

Sécurité physique et environnementale

Si des tiers stockent ou traitent des données confidentielles, leurs dispositifs de contrôle de sécurité physique et environnementale doivent répondre aux exigences de la politique de sécurité physique de Evalandgo Software.

Conformité et aspects juridiques

Evalandgo Software tiendra compte de toutes les réglementations et lois applicables lors de l'évaluation des fournisseurs et des tiers qui accèderont, stockeront, traiteront ou transmettront des données confidentielles de Evalandgo Software. Les évaluations de tiers doivent tenir compte des critères suivants :

- Protection des données clients et des dossiers de l'entreprise, conservation et destruction des dossiers.
- Confidentialité des données à caractère personnel.

Exceptions

Les demandes d'exception à la présente politique doivent être soumises à l'approbation du CEO.

Violations et application

Toute violation connue de la présente politique doit être signalée au responsable financier. Toute violation de la présente politique peut entraîner le retrait ou la suspension immédiats des privilèges système et réseau, et/ou une sanction disciplinaire conformément aux procédures de l'entreprise, pouvant aller jusqu'au licenciement.

Version	Date	Description	Auteur	Approuvé par
1.0	23-Fév-2024	Première version	Valentin Boschatel	Valérie Marusiak

