



Politique de sécurité de l'information

Responsable de la politique : Valentin Boschattel

Date d'entrée en vigueur : 14 février 2024

Vue d'ensemble

Cette politique de sécurité de l'information vise à protéger les employés et partenaires de Evalandgo Software ainsi que l'entreprise contre les actes illégaux ou préjudiciables commis sciemment ou non par d'autres personnes.

Les systèmes en lien avec l'Internet/Intranet/Extranet, y compris sans s'y limiter les équipements informatiques, les logiciels, les systèmes d'exploitation, les supports de stockage, les comptes réseau fournissant des e-mails, la navigation sur le Web et les transferts de fichiers, appartiennent à Evalandgo Software. Ces systèmes doivent être utilisés à des fins professionnelles et dans l'intérêt de l'entreprise et de nos clients dans le cadre d'opérations classiques.

La mise en place d'une sécurité optimale est le fruit d'un travail d'équipe impliquant la participation et le soutien de chaque employé ou sous-traitant de Evalandgo Software amené à utiliser des informations et/ou des systèmes d'information. Il incombe à chacun de lire et de comprendre cette politique, et de mener ses activités en conséquence.

Visée

Cette politique vise à communiquer nos politiques de sécurité de l'information et décrire l'utilisation acceptable et les mesures de protection des informations et des actifs de Evalandgo Software. Ces règles sont en place pour protéger les clients, les employés et Evalandgo Software. Une utilisation inappropriée expose Evalandgo Software à divers risques, y compris des attaques de virus, la compromission des systèmes et services réseau, des risques financiers et d'atteinte à la réputation, ainsi que des problèmes juridiques et de conformité.

La « Politique de sécurité de l'information » de Evalandgo Software se compose de la présente politique et de toutes les politiques de Evalandgo Software référencées dans ce document ou vers lesquelles il redirige.

Champ d'application

Cette politique s'applique à l'utilisation d'informations, d'appareils électroniques et informatiques, et de ressources réseau pour mener les activités de Evalandgo Software ou interagir avec des réseaux internes et des systèmes d'entreprise, qu'ils soient détenus ou loués par Evalandgo Software, l'employé ou un tiers. Il incombe à tous les employés, sous-traitants, consultants, intérimaires et autres collaborateurs de Evalandgo Software et de ses filiales de faire preuve de discernement en ce qui concerne l'utilisation appropriée des informations, des appareils électroniques et des ressources réseau conformément aux politiques et normes de Evalandgo Software, ainsi qu'aux lois et réglementations locales.

Cette politique s'applique aux employés, sous-traitants, consultants, intérimaires et autres collaborateurs de Evalandgo Software, y compris tout le personnel affilié à des tiers. Cette politique s'applique à toutes les données de l'entreprise et des clients dont Evalandgo Software est le responsable du traitement, ainsi qu'à tous les équipements, systèmes, réseaux et logiciels détenus ou loués par Evalandgo Software.

Signalement des incidents liés à la sécurité

Il est demandé à l'ensemble des utilisateurs de signaler les événements ou incidents connus ou présumés liés à la sécurité, y compris les violations des politiques et les lacunes observées en matière de sécurité. Les incidents doivent être signalés immédiatement ou dès que possible en envoyant un e-mail à : help@evalandgo.com.

Dans votre e-mail, veuillez décrire l'incident ou l'observation ainsi que tous les détails pertinents.

Dénonciation anonyme de fraudes

Notre politique de dénonciation a pour but d'encourager et de permettre aux employés et à d'autres personnes de faire part de leurs graves préoccupations en interne afin que nous puissions traiter et corriger les comportements et actions inappropriés. Il est de la responsabilité de tous les employés de signaler leurs préoccupations concernant les violations de notre code d'éthique ou les violations présumées de la loi ou des règlements qui régissent nos activités.

Il est contraire à nos valeurs que quiconque exerce des représailles à l'encontre d'un employé ou d'une personne qui, de bonne foi, signale une violation de l'éthique, ou une violation présumée de la loi, par exemple dans le cadre d'une plainte pour discrimination, d'une fraude présumée ou d'une violation présumée de tout règlement. Un employé qui exerce des représailles à l'encontre d'une personne qui a signalé une violation de bonne foi est passible de mesures disciplinaires pouvant aller jusqu'au licenciement.

Les dénonciations anonymes peuvent être soumises par le biais d'un courrier au service des ressources humaines.

Politique concernant les appareils mobiles

Tous les appareils des utilisateurs finaux (téléphones portables, tablettes, ordinateurs portables, ordinateurs de bureau, etc.) doivent être conformes à cette politique. Faites preuve d'une extrême prudence lorsque vous ouvrez les pièces jointes d'e-mails provenant d'expéditeurs inconnus, car elle peuvent contenir des logiciels malveillants.

Les mots de passe au niveau du système et de chaque utilisateur doivent être conformes à la politique de contrôle des accès. Il est interdit de communiquer ses accès à une autre personne, que ce soit intentionnellement ou par manque de sécurisation d'un appareil.

Tous les appareils auxquels l'utilisateur a recours pour accéder aux systèmes d'information (c'est-à-dire, aux e-mails) de Evalandgo Software doivent respecter les règles et exigences suivantes :

- Les appareils doivent être verrouillés à l'aide d'un écran de veille ou d'un écran verrouillé protégé par un mot de passe (ou un contrôle équivalent tel que le contrôle biométrique) après 10 minutes d'inactivité.
- Les appareils doivent être verrouillés chaque fois qu'ils sont laissés sans surveillance
- Les utilisateurs doivent signaler immédiatement toute suspicion d'utilisation abusive ou de vol d'un appareil mobile au service informatique de Evalandgo Software
- Les informations confidentielles ne doivent pas être stockées sur des appareils mobiles ou des clés USB (cela ne concerne pas les coordonnées professionnelles, p. ex., les noms, numéros de téléphone et adresses e-mail)

- Aucun appareil mobile utilisé pour accéder aux ressources de l'entreprise (comme les partages de fichiers et les e-mails) ne peut être partagé avec une autre personne.
- En cas de résiliation du contrat de travail, les utilisateurs acceptent de renvoyer tous les appareils appartenant à l'entreprise, et de supprimer l'ensemble des informations et comptes de l'entreprise de leurs appareils personnels

Politique de bureau et d'écran vides

Les utilisateurs ne doivent pas laisser de documents confidentiels non sécurisés sur leur bureau ou leur espace de travail, et doivent s'assurer que les écrans sont verrouillés lorsqu'ils ne sont pas utilisés.

Travail à distance et politique d'accès

Le télétravail fait référence à toute situation dans laquelle le personnel de l'entreprise opère à partir de lieux situés en dehors du bureau. Cela inclut le travail à distance, les lieux de travail flexibles, les environnements de travail virtuels et la télémaintenance. Les ordinateurs portables et autres ressources informatiques utilisées pour accéder au réseau de Evalandgo Software doivent être conformes aux exigences de sécurité décrites dans les politiques de sécurité de l'information de Evalandgo Software et respecter les normes suivantes :

- Les règles de l'entreprise doivent être suivies en cas de télétravail, y compris les protocoles de bureau vide, l'impression, la mise au rebut d'actifs et le signalement des événements de sécurité de l'information, afin d'éviter toute mauvaise manipulation ou toute exposition accidentelle d'informations sensibles.
- Pour veiller à ce qu'aucun appareil mobile compromis ne soit connecté au réseau de l'entreprise, les politiques en matière d'antivirus nécessitent l'utilisation d'un logiciel antivirus côté client.
- Le logiciel antivirus doit être configuré pour détecter et empêcher ou mettre en quarantaine les logiciels malveillants, effectuer des analyses périodiques du système et activer les mises à jour automatiques.
- Rendre obligatoire l'utilisation d'un VPN lors de la transmission d'informations confidentielles sur un réseau Wi-Fi public, afin d'éviter toute interception ou attaque de type « man-in-the-middle ».
- Lorsque vous travaillez à partir d'un réseau domestique, assurez-vous que les paramètres Wi-Fi par défaut sont modifiés, tels que le nom, le mot de passe et l'accès administrateur.
- Pour l'administrateur système, il est conseillé de configurer un réseau professionnel avec un chiffrement WPA3 puissant ou a minima WPA2 avec un mot de passe robuste, et, si cela est possible, de configurer un VLAN dédié. De plus, le WPS (Wi-Fi Protected Setup) et l'UPnP (Universal Plug and Play) doivent être désactivés s'ils ne sont pas spécifiquement requis.
- Les utilisateurs ne doivent pas se connecter à un réseau externe sans qu'un pare-feu sécurisé et à jour soit configuré sur l'ordinateur portable.
- Il est interdit aux utilisateurs de modifier ou de désactiver les dispositifs de contrôles de sécurité de l'entreprise, par exemple en utilisant des pare-feux ou antivirus personnels sur les systèmes utilisés pour accéder aux ressources de Evalandgo Software.
- L'utilisation de logiciels et/ou de services d'accès à distance (p. ex., client VPN) est autorisée tant qu'elle est fournie par l'entreprise et configurée pour l'authentification multifacteur (MFA).
- Les technologies d'accès à distance non autorisées ne peuvent pas être utilisées ou installées sur un système de Evalandgo Software.
- Les utilisateurs doivent utiliser un VPN lors de la transmission d'informations confidentielles sur un réseau Wi-Fi public.
- Si vous accédez aux systèmes à partir d'un ordinateur public (p. ex. dans un centre d'affaires, un hôtel, etc.), déconnectez-vous de la session et n'enregistrez rien. Ne cochez pas la case « Se souvenir de moi », rassemblez tous les documents imprimés et ne téléchargez pas de fichiers sur un système sur lequel Evalandgo Software n'a pas de contrôle

Politique d'utilisation acceptable

Les informations propriétaires de Evalandgo Software et celles concernant ses clients stockées sur des appareils électroniques et informatiques, qu'ils soient détenus ou loués par Evalandgo Software, l'employé ou un tiers, demeurent la propriété exclusive de Evalandgo Software aux fins de cette politique. Les employés et les sous-traitants doivent s'assurer par des moyens juridiques ou techniques que les informations propriétaires sont protégées conformément à la politique de gestion des données. L'utilisation de Google Drive pour le stockage de fichiers professionnels est requise pour les utilisateurs d'ordinateurs portables ou d'appareils fournis par l'entreprise. La « sauvegarde » de votre ordinateur portable doit être effectuée en stockant les documents importants sur le système de partage de fichiers.

Il vous incombe de signaler rapidement le vol, la perte ou la divulgation non autorisée des équipements ou données propriétaires de Evalandgo Software. Vous pouvez accéder aux informations propriétaires de Evalandgo Software et les utiliser ou les partager uniquement dans la mesure où cela est autorisé et nécessaire dans le cadre de vos attributions. Les employés doivent faire preuve de discernement quant au caractère raisonnable de l'utilisation personnelle des appareils fournis par l'entreprise.

Pour des raisons de sécurité et de maintenance réseau, le personnel autorisé de Evalandgo Software peut surveiller l'équipement, les systèmes et le trafic réseau à tout moment.

Evalandgo Software se réserve le droit d'auditer régulièrement les réseaux et les systèmes afin de garantir le respect de cette politique.

Utilisation inacceptable

De manière générale, les activités ci-dessous sont interdites. Les employés peuvent être exemptés de ces restrictions dans le cadre de leurs responsabilités professionnelles légitimes avec l'approbation de la direction dûment documentée. Les employés de Evalandgo Software ne sont en aucun cas autorisés à prendre part à des activités illégales en vertu de la législation locale, étatique, fédérale ou internationale lors de l'utilisation de ressources appartenant à Evalandgo Software ou lorsqu'ils représentent Evalandgo Software à quelque titre que ce soit. La liste ci-dessous n'est pas exhaustive, mais tente de fournir un cadre pour les activités caractérisant une utilisation inacceptable.

Les activités suivantes sont strictement interdites, sans exception :

1. Violer les droits d'une personne ou d'une entreprise protégées par des droits d'auteur, un secret commercial, un brevet ou toute autre propriété intellectuelle, ou par des lois ou réglementations similaires, y compris sans s'y limiter installer ou diffuser des logiciels « piratés » ou d'autres logiciels dont l'utilisation n'est pas dûment autorisée par Evalandgo Software.
2. Procéder à la copie non autorisée de supports protégés par des droits d'auteur, y compris sans s'y limiter numériser et distribuer des photographies provenant de magazines, livres ou autres sources protégées par des droits d'auteur, de la musique protégée par des droits d'auteur, et installer des logiciels protégés par des droits d'auteur pour lesquels Evalandgo Software ou l'utilisateur final ne disposent pas de licence active.
3. L'accès aux données, à un serveur ou à un compte à d'autres fins que la poursuite des activités de Evalandgo Software, même si vous disposez d'un accès autorisé, est interdit.
4. L'exportation de logiciels, d'informations techniques, de logiciels de chiffrement ou de technologies en violation des lois régionales ou internationales sur le contrôle des exportations est illégale. Les dirigeants concernés doivent être consultés avant l'exportation de tout support de ce type.

5. Introduire des programmes malveillants au sein du réseau ou des systèmes (p. ex. virus, vers informatiques, chevaux de Troie, mail bombing, etc.).
6. Révéler le mot de passe de votre compte à d'autres personnes ou permettre à d'autres personnes d'utiliser votre compte. Cela inclut la famille et les autres membres du foyer en cas de télétravail.
7. Utiliser une ressource informatique de Evalandgo Software pour chercher activement à se procurer ou transmettre des supports contraires aux lois sur le harcèlement sexuel ou les environnements de travail hostiles.
8. Faire des offres frauduleuses de produits, d'articles ou de services à partir d'un compte appartenant à Evalandgo Software.
9. Formuler des déclarations expresses ou implicites concernant la garantie, sauf lorsque cela rentre dans le cadre des attributions liées au poste.
10. Introduire des failles de sécurité ou des perturbations au niveau des communications réseau. Les failles de sécurité incluent sans s'y limiter l'accès à des données dont l'employé n'est pas le destinataire prévu, ou la connexion à un serveur ou à un compte auquel l'employé n'est pas expressément autorisé à accéder, sauf si cela rentre dans le cadre de ses attributions. Aux fins de cette section, les « perturbations » incluent sans s'y limiter le reniflage réseau, les inondations ping, l'usurpation d'adresse IP, le déni de service et la falsification des informations de routage à des fins malveillantes.
11. Le balayage de ports est expressément interdit, sauf si l'équipe d'ingénierie de Evalandgo Software en est préalablement avertie.
12. Exécuter toute forme de surveillance du réseau qui interceptera des données non destinées à l'hôte de l'employé, sauf si cela rentre dans le cadre des attributions de l'employé.
13. Contourner l'authentification des utilisateurs ou la sécurité de tout hôte, réseau ou compte.
14. Introduire des pots de miel, des réseaux de miel ou toute technologie similaire sur le réseau de Evalandgo Software.
15. Interférer auprès d'un utilisateur autre que l'hôte de l'employé ou lui refuser l'accès au service (par exemple, attaque par déni de service).
16. Utiliser un programme/un script/une commande, ou envoyer des messages de quelque nature que ce soit, dans l'intention d'interférer avec la session d'un utilisateur ou de la désactiver, indépendamment des moyens mis en œuvre.
17. Fournir des listes ou des informations sur les employés, sous-traitants, partenaires ou clients de Evalandgo Software à des parties extérieures à Evalandgo Software sans autorisation.

Activités liées aux e-mails et à la communication

Lorsqu'ils ont recours aux ressources de l'entreprise pour accéder à Internet et l'utiliser, les utilisateurs doivent comprendre qu'ils représentent l'entreprise et agir en conséquence.

Les activités suivantes sont strictement interdites, sans exception :

1. L'envoi d'e-mails non sollicités, y compris l'envoi de « courriers indésirables » ou d'autres supports publicitaires à des personnes qui ne les ont pas spécifiquement demandés (spam) ;
2. Toute forme de harcèlement par e-mail, téléphone ou SMS, qu'elle soit caractérisée par le langage employé, la fréquence d'envoi ou la taille des messages ;
3. L'utilisation non autorisée ou la falsification de l'en-tête des e-mails ;
4. La sollicitation d'e-mails pour toute autre adresse e-mail que celle du compte de l'intervenant, à des fins de harcèlement ou de collecte de réponses ;
5. La création ou le transfert de « chaînes d'e-mails », de « systèmes de Ponzi » ou de tout autre type de « ventes pyramidales » ;
6. L'utilisation d'e-mails non sollicités provenant de réseaux de Evalandgo Software ou émanant d'autres prestataires de services agissant au nom de Evalandgo Software, ou dans le but de faire la publicité de tout service hébergé par Evalandgo Software ou connecté via son réseau.

Politiques et procédures supplémentaires incorporées par référence

Les membres du personnel sont tenus de lire et respecter toutes les politiques relatives à leurs rôles et responsabilités.

Rôle	Visée
Politique de contrôle des accès	Limiter l'accès aux systèmes d'information et de traitement des informations, réseaux et installations aux seules parties autorisées conformément aux besoins de l'entreprise.
Politique de gestion des actifs	Identifier les actifs de l'entreprise et les protéger en définissant les responsabilités adéquates.
Plan de continuité des activités et de reprise après sinistre	Préparer Evalandgo Software en cas d'interruption de service prolongée causée par des facteurs échappant à notre contrôle (p. ex., catastrophes naturelles, événements d'origine humaine) et rétablir les services dans la mesure du possible dans un délai minimal.
Politique de cryptographie	Garantir une utilisation correcte et efficace de la cryptographie pour protéger la confidentialité, l'authenticité et/ou l'intégrité des informations.
Politique de gestion des données	Garantir que les informations sont classées et protégées selon leur importance pour l'entreprise.
Politique en matière de ressources humaines	S'assurer que les employés et les sous-traitants répondent aux exigences de sécurité, comprennent leurs responsabilités et conviennent à leur rôle.
Plan de réponse aux incidents	Politique et procédures pour les incidents présumés ou confirmés liés à la sécurité de l'information.
Politique de sécurité des opérations	Assurer le fonctionnement correct et sécurisé des systèmes et installations de traitement de l'information.
Politique de sécurité physique	Empêcher tout accès physique non autorisé ou tout dommage aux informations et aux installations de traitement de l'information de l'entreprise.
Politique de gestion des risques	Définir le processus d'évaluation et de gestion des risques de sécurité de l'information de Evalandgo Software afin d'atteindre les objectifs de l'entreprise en matière de sécurité de l'information et d'activité.
Politique de développement sécurisé	Veiller à ce que la sécurité de l'information soit conçue et mise en œuvre pendant le cycle de développement des applications et des systèmes d'information.
Politique de gestion des tiers	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.

Respect de la politique

Evalandgo Software évaluera et contrôlera la conformité à la présente politique par le biais de diverses méthodes incluant, sans s'y limiter, un suivi continu et des audits internes et externes.

Exceptions

Les demandes d'exception à cette politique doivent être soumises à l'approbation du responsable informatique.

Violations et application

Toute violation connue de cette politique doit être signalée au responsable informatique. Toute violation de cette 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	14-Fev-2024	Première version	Valentin Boschattel	Valérie Marusiak