



Politique de contrôle des accès

Responsable de la politique : CEO

Date d'entrée en vigueur : 23 Février 2024

Visée

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.

Champ d'application

Tous les systèmes d'information de Evalandgo Software qui traitent, stockent ou transmettent des données confidentielles conformément à la Politique de gestion des données de Evalandgo Software. Cette politique s'applique à tous les employés de Evalandgo Software et à toutes les parties externes ayant accès aux réseaux et aux ressources système de Evalandgo Software.

Politique

L'accès aux ressources informatiques est limité au seul personnel ayant besoin d'y accéder dans le cadre de ses fonctions. Les droits d'accès doivent être accordés ou révoqués conformément à la présente Politique de contrôle des accès.

Besoins professionnels pour le contrôle des accès

Politique de contrôle des accès

Evalandgo Software déterminera le type et le niveau d'accès accordés à chaque utilisateur conformément au « principe du moindre privilège ». Ce principe stipule que les utilisateurs bénéficient uniquement du niveau d'accès absolument requis pour exécuter leurs fonctions professionnelles, sur la base des besoins professionnels et de sécurité de Evalandgo Software. Les autorisations et droits d'accès non expressément accordés sont, par défaut, interdits.

La principale méthode utilisée par Evalandgo Software pour accorder et gérer des contrôles d'accès et des droits d'accès cohérents consiste à mettre en œuvre le contrôle d'accès basé sur les rôles (RBAC). Dans la mesure du possible, les droits et les restrictions doivent être attribués à des groupes. Les comptes d'utilisateurs individuels peuvent se voir accorder des autorisations supplémentaires si nécessaire, avec l'approbation du propriétaire du système ou de la partie autorisée.

Tous les accès privilégiés à l'infrastructure de production doivent utiliser l'authentification multifacteur (MFA).

Accès aux réseaux et aux services réseau

Les normes de sécurité suivantes régissent l'accès aux réseaux et aux services réseau de Evalandgo Software :

- L'accès technique aux réseaux de Evalandgo Software doit être formellement documenté, en incluant notamment le rôle standard ou l'approbateur, le fournisseur de l'autorisation et la date.
- Seuls les employés autorisés de Evalandgo Software et les tiers, dans le cadre d'un contrat ou d'un cahier des charges signé, et sous réserve de l'existence d'un besoin professionnel, doivent avoir accès aux réseaux et ressources de production de Evalandgo Software.
- Les invités de Evalandgo Software peuvent être autorisés à accéder aux réseaux invités sans demande documentée après s'être inscrits auprès du personnel administratif.
- Les connexions distantes aux réseaux et aux systèmes de production doivent être chiffrées.

Gestion de l'accès client

Lorsque vous configurez un accès inter-comptes à l'aide de rôles IAM d'AWS, vous devez utiliser une valeur que vous générez pour l'identifiant externe, plutôt qu'une valeur fournie par le client, afin de garantir l'intégrité de la configuration du rôle inter-comptes. Un identifiant externe généré par un partenaire garantit que les parties malveillantes ne peuvent pas usurper la configuration d'un client et assure l'unicité et la cohérence du format pour l'ensemble des clients.

Les identifiants externes utilisés doivent être uniques pour chaque client. La réutilisation d'identifiants externes pour différents clients ne résout pas le problème confus des adjoints et fait courir le risque que le client A puisse consulter les données du client B en utilisant l'ARN du rôle du client B avec l'identifiant externe du client B.

Les clients ne doivent pas pouvoir définir ou influencer les identifiants externes. Lorsque l'identifiant externe est modifiable, un client peut usurper la configuration d'un autre client.

Gestion des accès utilisateur

Evalandgo Software exige que tout le personnel dispose d'un identifiant utilisateur unique pour l'accès aux systèmes, et que les informations d'identification et les mots de passe des utilisateurs ne soient pas partagés entre plusieurs membres du personnel. Dans la mesure du possible, les utilisateurs disposant de plusieurs niveaux d'accès (par ex. les administrateurs) doivent disposer de comptes distincts pour l'utilisation normale des systèmes et pour les fonctions d'administration. Les comptes root, de service et administrateur peuvent utiliser un système de gestion des mots de passe pour partager les mots de passe uniquement à des fins de continuité des activités. Les administrateurs utiliseront des comptes administrateur partagés uniquement lorsque cela s'avère nécessaire. Les administrateurs ne doivent utiliser les comptes administratifs partagés qu'en cas de besoin. Si un mot de passe est compromis ou présumé compromis, l'incident doit être immédiatement signalé à l'équipe de réponse aux incidents, et le mot de passe doit être modifié.

Enregistrement et suppression d'utilisateurs

Seuls les administrateurs autorisés peuvent créer de nouveaux identifiants utilisateur, et ce uniquement après réception d'une demande documentée de la part de parties autorisées. Les demandes de création de comptes utilisateur doivent s'accompagner d'une autorisation des propriétaires des données ou d'un responsable de Evalandgo Software autorisé à accorder un accès au système. Avant la création du compte, les administrateurs devront s'assurer que le compte n'enfreint aucune politique de sécurité ou de contrôle des accès au système de Evalandgo Software, telle que la séparation des tâches, les mesures de prévention des fraudes ou les restrictions relatives aux droits d'accès.

Les identifiants utilisateur doivent être rapidement désactivés ou supprimés lorsque les utilisateurs associés quittent l'entreprise ou que leur contrat prend fin, conformément aux accords de niveau de service. Les identifiants utilisateur ne doivent pas être réutilisés.

Attribution des accès

- Les nouveaux employés et/ou sous-traitants ne doivent pas avoir accès aux systèmes de production de Evalandgo Software tant qu'ils n'ont pas achevé l'ensemble des tâches d'intégration des RH, lesquelles peuvent inclure, sans s'y limiter, la signature du contrat de travail, de l'accord sur la propriété intellectuelle et de la reconnaissance de la politique de sécurité de l'information de Evalandgo Software.
- L'accès doit être limité aux seules ressources nécessaires à l'utilisateur pour exécuter ses fonctions professionnelles
- Aucun accès ne peut être accordé avant la date de début officielle du contrat de l'employé
- Les demandes d'accès et les modifications de droits d'accès doivent être documentées dans un ticket de demande d'accès ou un e-mail. Aucune autorisation ne sera accordée sans l'approbation du propriétaire du système ou des données, ou de la direction
- Les enregistrements des modifications d'autorisations et de privilèges doivent être conservés pendant au moins trois ans

Gestion des accès privilégiés

Evalandgo Software doit veiller à ce que l'attribution et l'utilisation des droits d'accès privilégiés soient restreintes et gérées judicieusement. L'objectif est de garantir que seuls les utilisateurs, composants logiciels et services autorisés bénéficient de droits d'accès privilégiés. Evalandgo Software garantira que l'accès et les privilèges sont conformes à la norme suivante :

- Identifier et valider les utilisateurs : identifiez les utilisateurs qui ont besoin d'un accès privilégié pour chaque système et processus.
- Allouer des droits privilégiés : accordez des droits d'accès en basant les attributions sur des besoins et des compétences spécifiques, et en respectant strictement la politique de contrôle d'accès.
- Maintenir les protocoles d'autorisation : documentez toutes les attributions d'accès privilégié.
- Appliquer une authentification forte : exigez une MFA (authentification multifacteur) pour tous les accès privilégiés.
- Empêcher l'utilisation d'identifiants d'administrateur génériques : empêchez l'utilisation d'identifiants d'administration génériques
- Adopter des protocoles d'accès à durée limitée : accordez un accès privilégié uniquement pour la durée nécessaire de réalisation de tâches spécifiques et révoquez-les une fois la tâche terminée.
- Garantir la journalisation et l'audit : consignez toutes les connexions et activités privilégiées
- Distinguer et séparer les identités : préservez des identités distinctes pour les droits d'accès privilégiés et assurez-vous que ces identités ne sont ni partagées entre plusieurs utilisateurs ni utilisées pour des tâches de routine non administratives.

Évaluation des accès utilisateur

Les administrateurs doivent procéder à des évaluations des droits d'accès des comptes utilisateur, administrateur et de service chaque trimestre afin de s'assurer que l'accès accordé aux utilisateurs est restreint aux seuls systèmes requis pour exécuter leurs fonctions. Les évaluations des accès doivent être documentées.

Les évaluations des accès peuvent inclure l'appartenance à un groupe ainsi que des évaluations de toute autorisation spécifique ou basée sur une exception. Les droits d'accès devront également être évalués suite à tout changement de poste, y compris la promotion, la rétrogradation ou le transfert au sein de l'entreprise.

Suppression et modification des droits d'accès

Les droits d'accès de tous les utilisateurs seront rapidement supprimés en cas de résiliation du contrat de travail, ou lorsque ces droits ne sont plus nécessaires en raison d'un changement de

fonction ou de poste. Le délai maximal autorisé pour la révocation de l'accès est de 24 heures ouvrables.

Procédure d'attribution, de révocation et de modification des accès

La procédure de gestion des accès applicable aux systèmes de Evalandgo Software est disponible à l'annexe A de cette politique.

Séparation des tâches

Les tâches conflictuelles et les domaines de responsabilité doivent être séparés afin de réduire les possibilités de modification non autorisée ou non intentionnelle ou d'utilisation abusive des actifs d'Evalandgo Software. Lors de l'attribution de l'accès, il faut veiller à ce qu'aucune personne ne puisse accéder, modifier ou utiliser les actifs sans autorisation ou détection. L'initiation d'un événement doit être séparée de son autorisation. La possibilité de collusion doit être prise en compte lors de la sélection des niveaux d'accès pour les individus et les groupes.

Responsabilité des utilisateurs en matière de gestion des informations d'authentification secrètes

Le contrôle et la gestion des mots de passe d'utilisateurs individuels relèvent de la responsabilité de l'ensemble du personnel de Evalandgo Software et des utilisateurs tiers. Les utilisateurs doivent protéger les informations d'authentification secrètes conformément à la Politique de sécurité de l'information.

Politique de mot de passe

Dans la mesure du possible, les mots de passe de systèmes confidentiels doivent contenir au moins 12 caractères :

- une majuscule, un chiffre
- Les mots de passe expirent après 90 jours
- Lors d'une réinitialisation manuelle de mot de passe, l'identité d'un utilisateur doit être vérifiée avant de modifier le mot de passe
- Ne limitez pas les caractères autorisés pouvant être utilisés
- Ne limitez pas la longueur du mot de passe à une valeur inférieure à 64 caractères
- N'utilisez pas de questions secrètes (lieu de naissance, etc.) comme seule exigence de réinitialisation du mot de passe
- Exigez la vérification par e-mail d'une demande de changement de mot de passe
- Exigez le mot de passe actuel en plus du nouveau mot de passe lors du changement de mot de passe
- Vérifiez régulièrement que les mots de passe des utilisateurs existants ne sont pas compromis

Accès aux systèmes et aux applications

Restriction de l'accès aux informations

Les applications doivent restreindre l'accès aux fonctions et informations du programme aux seuls utilisateurs autorisés et au personnel d'assistance conformément à la politique de contrôle des accès définie. Le niveau et le type de restrictions appliqués par chaque application doivent être basés sur les exigences individuelles de chacune, telles qu'identifiées par le propriétaire des données. La politique de contrôle des accès propre à l'application doit également être conforme aux politiques de Evalandgo Software concernant les contrôles d'accès et la gestion des données.

Avant la mise en œuvre, les critères d'évaluation pertinents doivent être appliqués aux applications afin de déterminer les contrôles d'accès et les politiques de données nécessaires. Les critères d'évaluation incluent sans s'y limiter :

- La sensibilité et la classification des données
- Le risque d'accès non autorisé ou de divulgation des données
- La possibilité de contrôler les droits d'accès des utilisateurs à l'application et aux données stockées dans celle-ci, ainsi que la précision des contrôles
- Les restrictions applicables aux sorties de données, y compris le filtrage des informations sensibles, le contrôle des sorties et la restriction de l'accès aux informations au seul personnel autorisé
- Le contrôle des droits d'accès entre l'application évaluée et d'autres applications et systèmes
- Les restrictions de programmation concernant l'accès des utilisateurs aux fonctions des applications et aux instructions privilégiées
- Les fonctionnalités de journalisation et d'audit des fonctions du système et de l'accès aux informations
- Les fonctionnalités de conservation et de déplacement des données qui ne sont plus utilisées

Tous les comptes par défaut non nécessaires doivent être supprimés ou désactivés avant de rendre un système disponible sur le réseau. Plus précisément, les mots de passe et les informations d'identification par défaut des fournisseurs doivent être modifiés sur tous les systèmes, appareils et infrastructures de Evalandgo Software avant le déploiement. Cela s'applique à TOUS les mots de passe par défaut, ce qui inclut sans s'y limiter les mots de passe utilisés par les systèmes d'exploitation, les logiciels qui fournissent des services de sécurité, les comptes d'application et de système, et les chaînes de communauté SNMP (Simple Network Management Protocol) lorsque cela est possible.

Procédures de connexion sécurisée

Les contrôles de connexion sécurisée sont conçus et sélectionnés conformément à la sensibilité des données et au risque d'accès non autorisé, sur la base de la totalité de l'architecture de sécurité et de contrôle d'accès.

Système de gestion des mots de passe

Les systèmes de gestion des mots de passe doivent être interactifs et aider le personnel d'Evalandgo Software à garantir le respect continu des normes relatives aux mots de passe en appliquant des critères de robustesse tels que la longueur minimale et la complexité du mot de passe lorsque cela est possible.

Le stockage et la transmission des mots de passe doivent être strictement protégés au moyen des mesures de protection cryptographiques appropriées, soit par hachage, soit par chiffrement.

Accès au code source du programme

L'accès au code source du programme et aux éléments associés, y compris aux conceptions, spécifications, plans de vérification et plans de validation, doit être strictement contrôlé afin d'empêcher l'intégration de fonctionnalités non autorisées au logiciel, d'éviter les modifications involontaires et de protéger la propriété intellectuelle de Evalandgo Software.

Tout accès au code source doit être fondé sur les besoins professionnels et doit être consigné à des fins d'évaluation et d'audit.

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 rapportée au responsable informatique. Les violations de la présente politique sont susceptibles d'entraîner le retrait ou la suspension immédiats des privilèges sur le système et le réseau et/ou des mesures disciplinaires conformément aux procédures en place dans l'entreprise, y compris la résiliation du contrat de travail.

Version	Date	Description	Auteur	Approuvé par
1.0	23-Fév-2024	Première version	Hugo Bachelet	Valentin Boschattel
1.1	18-Mar-2025	Deuxième version	Hugo Bachelet	Valentin Boschattel

ANNEXE A - Procédure de gestion des accès

À l'issue du processus d'intégration, les RH enverront un e-mail qui générera une série de tickets de service relatifs à l'accès.

Le service informatique fournira l'accès à tous les systèmes de l'entreprise ainsi qu'aux systèmes d'ingénierie pour les membres du personnel technique.

Tout accès supplémentaire, au-delà de l'accès préapprouvé standard, doit être demandé et approuvé par un responsable ou le propriétaire du système.

ANNEXE B — Matrice d'accès

Rôle	E-mails	Google Workspace	Outil de dépenses	GRC	Appli	Infrastructure	Contrôle des versions	Système de conception	Analyse de vulnérabilité
développeur	x	x			x		x	x	
responsable développeur	x	x		x	x	x	x	x	x
Technicien réseau / cybersécurité	x	x		x		x			x
Support client	x	x			x				
Responsable marketing	x	x	x		x				
Ressources humaines	x	x	x						