



Politique de développement sécurisé

Responsable de la politique : **CEO**

Date d'entrée en vigueur : 23 Février 2024

Nom de l'entreprise :	Evalandgo Software	
Responsables de la politique :	Valérie Marusiak, CEO	Téléphone :
Date d'entrée en vigueur :	23 Février 2024	Date de révision : 23 Février 2024
Dernier avis :	23 Février 2024	Prochaine révision : 23 Février 2025

Visée

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.

Champ d'application

Toutes les applications et tous les systèmes d'information de **Evalandgo Software** qui sont essentiels à ses activités et/ou qui utilisent, stockent ou transmettent des données confidentielles. La présente politique s'applique à tous les ingénieurs et développeurs internes et externes des logiciels et de l'infrastructure de Evalandgo Software.

Politique

La présente politique décrit les règles d'acquisition et de développement de logiciels et de systèmes qui sont à appliquer aux développements au sein de Evalandgo Software.

Procédures de contrôle des modifications système

Les modifications apportées aux systèmes au cours du cycle de développement doivent être contrôlées par l'utilisation de procédures formelles de contrôle des modifications. Les procédures et exigences de contrôle des modifications sont décrites dans la politique de sécurité des opérations de Evalandgo Software.

Les modifications importantes de code doivent être examinées et approuvées par **le responsable développeurs** avant d'être intégrées à tout domaine de production.

Les procédures de contrôle des modifications doivent veiller à ce que le développement, les tests et le déploiement des modifications ne soient pas effectués par une seule personne sans approbation et supervision.

Contrôle des versions des logiciels

Tous les logiciels de Evalandgo Software sont soumis à un contrôle des versions et synchronisés entre les contributeurs (développeurs). L'accès au référentiel central est limité selon la fonction occupée par l'employé. L'intégralité du code est écrite, testée et enregistrée dans un référentiel local avant d'être synchronisé avec le référentiel d'origine.

Évaluation technique des applications après modification de la plateforme d'exploitation

Lorsque les plateformes d'exploitation sont modifiées, les applications essentielles doivent être évaluées et testées pour s'assurer qu'il n'y a pas d'impact négatif sur les opérations ou la sécurité de l'entreprise.

Restrictions à l'apport de modifications aux packages logiciels

Nous ne recommandons pas d'apporter des modifications à des packages d'applications métier tiers : il convient de les limiter aux modifications nécessaires et d'opérer un contrôle strict de toutes les modifications.

Principes d'ingénierie de systèmes sécurisés

Des principes d'ingénierie de systèmes sécurisés doivent être établis, documentés, maintenus à jour et appliqués lors de toute action d'implémentation des systèmes d'information.

Au minimum, les principes de sécurité par la conception et de confidentialité par la conception suivants doivent être appliqués :

Principes de sécurité par la conception :

1. Minimiser la surface d'attaque
2. Établir des valeurs par défaut sécurisées
3. Principe de moindre privilège
4. Principe de défense en profondeur
5. Sûreté intégrée
6. Confiance zéro
7. Séparation des tâches
8. Éviter la sécurité par l'obscurité
9. Simplifier la sécurité
10. Corriger correctement les problèmes de sécurité

Principes de protection de la vie privée dès la conception :

1. Proactivité plutôt que réactivité, prévention plutôt que correction
2. La confidentialité comme paramètre par défaut
3. La confidentialité intégrée à la conception

4. Fonctionnalité complète - somme positive plutôt que somme nulle
5. Sécurité de bout en bout - protection tout au long du cycle de vie
6. Visibilité et transparence - adopter une approche ouverte
7. Respect de la vie privée des utilisateurs - l'utilisateur avant tout

Les développeurs de logiciels doivent respecter les normes de codage de Evalandgo Software tout au long du cycle de développement, y compris les normes de qualité, de commentaires et de sécurité.

Environnement de développement sécurisé

Evalandgo Software doit établir et protéger de manière appropriée les environnements des actions de développement et d'intégration des systèmes qui couvrent l'ensemble du cycle de développement des systèmes. Les environnements suivants doivent faire l'objet d'une séparation logique ou physique :

- Production
- Test/pré-production
- Développement

Développement externalisé

Evalandgo Software doit superviser et surveiller l'activité externalisée de développement de systèmes. Le développement externalisé doit respecter toutes les normes et les politiques de Evalandgo Software.

Tests de sécurité du système

Des tests de bon fonctionnement de la sécurité doivent être effectués à des périodes définies pendant le cycle de développement. Aucun code ne doit être déployé sur les systèmes en production de Evalandgo Software sans disposer de résultats de tests réussis et documentés et de preuves des activités de correction en matière de sécurité.

Gestion des vulnérabilités des applications

Le code d'application doit être analysé avant le déploiement. Les correctifs visant à corriger les vulnérabilités des applications qui ont un impact significatif sur la sécurité doivent être déployés dans les 90 jours suivant la découverte.

Tests d'acceptation du système

Des programmes de tests d'acceptation et les critères associés doivent être établis pour les nouveaux systèmes d'information, les mises à niveau et les nouvelles versions.

Avant de déployer le code correspondant, une liste de contrôle DOIT être remplie. Celle-ci couvre tous les plans de test démontrant la bonne réalisation de tous les tests associés et la correction des problèmes identifiés.

Protection des données de test

Les données de test doivent être sélectionnées avec soin, protégées et contrôlées. Les données confidentielles des clients doivent être protégées conformément à tous les contrats et engagements. Les données clients ne doivent pas être utilisées à des fins de tests sans l'autorisation explicite du propriétaire des données et du **responsable informatique et sécurité**.

Acquisition de systèmes et de logiciels tiers

L'acquisition de systèmes et de logiciels tiers doit s'effectuer conformément aux exigences de la Politique de gestion des tiers de Evalandgo Software.

Formation des développeurs

Les développeurs de logiciels doivent bénéficier d'une formation de développement sécurisée adaptée à leur rôle au moins une fois par an. Le contenu de la formation est déterminé par la direction mais doit aborder la prévention des attaques et vulnérabilités courantes des applications Web. Les menaces et vulnérabilités suivantes doivent être traitées le cas échéant :

- Prévention des attaques par contournement d'autorisation ;
- Prévention de l'utilisation d'identifiants de session non sécurisés ;
- Prévention des attaques par injection ;
- Prévention des attaques par cross-site scripting ;
- Prévention des attaques par falsification des requêtes intersites ;
- Prévention de l'utilisation de bibliothèques vulnérables.

Exceptions

Les demandes d'exception à la présente politique doivent être soumises au **responsable informatique et sécurité** pour approbation.

Violations et application

Toute violation connue de la présente politique doit être signalée **responsable informatique et sécurité**. 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	23-Fév-2024	Première version	Hugo Bachelet	Valentin Boschattel