



Politique de cryptographie

Responsable de la politique : Responsable informatique et sécurité

Date d'entrée en vigueur : 23 Février 2024

Visée

Garantir une utilisation correcte et efficace des méthodes de chiffrement pour protéger la confidentialité, l'authenticité et/ou l'intégrité des informations. Cette politique établit les exigences relatives à l'utilisation et la protection des clés de chiffrement et des méthodes cryptographiques tout au long du cycle de vie du chiffrement.

Champ d'application

Tous les systèmes d'information développés et/ou contrôlés par Evalandgo Software qui stockent ou transmettent des données confidentielles.

Politique

Evalandgo Software doit évaluer les risques inhérents au traitement et au stockage des données, et mettre en œuvre des méthodes de chiffrement pour atténuer ces risques lorsque cela est jugé approprié. Lorsque le chiffrement est utilisé, une méthode robuste ainsi que les processus et procédures de gestion des clés associés doivent être mis en œuvre et documentés. L'intégralité du chiffrement doit être effectué conformément aux normes de l'industrie, y compris la publication NIST SP 800-57.

Les données du client ou les données confidentielles de l'entreprise doivent utiliser des chiffrements forts et des configurations conformes aux recommandations des fournisseurs et aux meilleures pratiques de l'industrie, notamment [NIST, lorsqu'elles sont stockées ou transférées sur un réseau public.](#)

Gestion des clés

L'accès aux clés et aux secrets doit être rigoureusement contrôlé conformément à la Politique de contrôle des accès.

Le tableau suivant inclut l'utilisation recommandée des clés de chiffrement :

Domaine	Type de clé	Algorithme	Longueur de la clé	Expiration maximale
Certificat Web	RSA ou ECC avec signature SHA2+	RSA ou ECC avec signature SHA2+	2 048 bits ou supérieur/RSA, 256 bits ou supérieur/ECC	Jusqu'à 1 an

Chiffrement Web (TLS)	Chiffrement asymétrique	Chiffrements de niveau B ou supérieur à l'évaluation SSL Labs	Variable	N/A
Données confidentielles statiques	Chiffrement symétrique	AES	256 bits	1 an
Mots de passe	Hachage à sens unique	Bcrypt, PBKDF2, ou scrypt, Argon2	256 bits + étirement 10K. Inclure un sel + poivre cryptographiques uniques	N/A
Stockage des terminaux (SSD/HDD)	Chiffrement symétrique	AES	128 ou 256 bits	N/A

Exceptions

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

Une exception documentée est requise avant de déplacer, copier ou stocker des données confidentielles du client ou de l'entreprise sur tout support ou dispositif amovible ; tous les appareils portables et les supports amovibles contenant des données sensibles doivent être chiffrés à l'aide de normes et de mécanismes approuvés.

Violations et application

Toute violation connue de cette politique doit être signalée au 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	Valentin Boschattel	Valérie Marusiak