DiliTrust

La sécurité chez DiliTrust

La sécurité de vos données est notre priorité

Nos clients nous confient leurs informations les plus stratégiques : nous leur devons le plus haut niveau de sécurité. La sécurité de vos données est cruciale pour la pérennité de votre organisation. Le vol ou la perte de données, la non-conformité avec les exigences réglementaires tels que le RGPD, ou encore le coût engendré par la perte de temps due à une interruption de service peuvent infliger des dommages considérables à toute entreprise.

La sécurité de vos données est vitale pour vous ; elle l'est encore plus pour nous.

Qu'il s'agisse de se protéger contre les piratages externes, les failles de sécurité internes, la divulgation d'information ou l'erreur humaine, la sécurité est essentielle pour nos clients et celle-ci fait partie intégrante de notre service. Notre organisation toute entière est focalisée sur cet objectif : vous offrir le plus haut niveau de sécurité possible.

Une culture de la sécurité

DiliTrust est certifiée ISO 27001:2017, ISO 27701:2019 et SOC 2. Ces normes internationales spécifient des exigences relatives aux bonnes pratiques sur la gestion de la sécurité de l'information ainsi que sur la gestion des données à caractère personnel. Leur périmètre est très étendu et va au-delà des exigences en matière de protection, de confidentialité ou encore des enjeux techniques ou de sécurité. De plus, tous nosemployés sont formés au respect de ces normes.

Infrastructure

Emplacement des serveurs

Nos serveurs répondent aux normes de sécurité les plus strictes et **sont situés exclusivement dans la région de nos clients** : en Europe pour les clients de l'UE, au Canada pour les clients canadiens, au Canada ou en Europe pour les clients d'Amérique latine, au Moyen-Orient, en Afrique ou au Maroc pour les clients de la région MEA et aux États-Unis pour les clients américains.

Les données hébergées ne sont jamais partagées avec des tiers et ne sont en aucun cas soumises à des lois extraterritoriales, garantissant à nos clients un contrôle total sur leurs informations sensibles à tout moment.

Sécurité physique

Un autre aspect important de la sécurité des données est la sécurité physique. L'accès physique au centre de données est contrôlé par un système de badge, de surveillance vidéo et de personnel sur place 24/7.

Les locaux sont équipés de systèmes de détection de fumée et d'un système de double alimentation systématique avec des génératrices de secours ayant une autonomie initiale de 48 heures. De plus, les locaux sont équipés de deux connexions réseau redondantes **afin d'éviter la dépendance à un seul fournisseur internet**.

De plus, toutes les installations sont protégées contre les inondations, les incendies et autres risques environnementaux.

Hébergement ultra sécurisé

Pour améliorer en permanence la protection des données et garantir la confidentialité de toutes les informations, tous les systèmes et données de DiliTrust sont hébergés sur des serveurs qui ont obtenu les plus hautes certifications internationales dans le domaine de la sécurité informatique. **L'hébergement est aussi certifié par la norme ISO/IEC 27001**. Cette norme garantit la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI) pour la sécurité des données.

ISO 27001 définit également des mesures de contrôle pour assurer la capacité des systèmes à fournir à nos clients le plus haut niveau de sécurité.

Contrôle et surveillance 24/7

Nos systèmes sont sous surveillance 24 heures sur 24, 7 jours sur 7, notamment contre toute tentative d'attaque ou la survenance d'un événement technique :

- Surveillance du matériel (taux d'utilisation de la mémoire RAM, des CPUs et du stockage), surveillance des performances applicatives ;
- Déclenchement automatique d'alertes en cas de détection d'activités suspectes ;
- EDR, Firewall, IDS (Intrusion Detection System),
- Système anti-flood (DDoS) et protection contre les attaques en force brute.

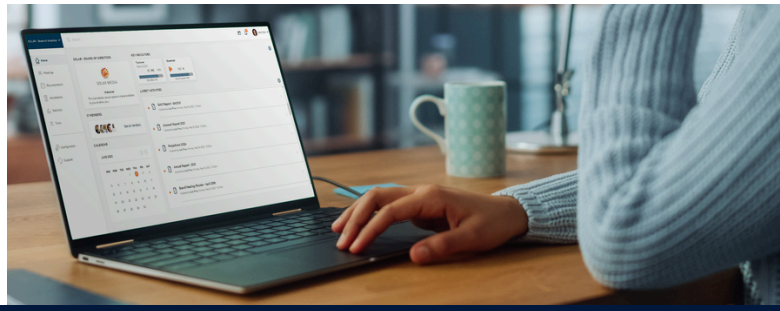
Tous les serveurs ont des disques et des **accès réseau redondants**, ainsi qu'un système de sauvegardes quotidiennes.

Sauvegardes

Les sauvegardes de l'ensemble du système sont effectuées chaque jour et stockées dans un emplacement secondaire géographiquement distant sous les mêmes conditions de sécurité que les serveurs de production et dans le même pays (donc sous la même juridiction).

Les sauvegardes sont conservées pendant sept jours glissants, puis **détruites définitivement** sans possibilité de récupération. Exemple : le fichier de sauvegarde du lundi efface automatiquement le fichier du lundi précédent.

Une installation secondaire opérationnelle est à disposition, en cas de force majeure, pour redémarrer le service (moyennant le temps de propagation DNS).



Chiffrement

Données au repos : AES 256

Toutes les données confidentielles au repos sont chiffrées en AES (Advanced Encryption Standard, Rijndael) avec une clé 256 bits, **le plus haut standard de chiffrement actuel**.

À la fois sur les serveurs et sur les appareils mobiles (pour les données stockées localement).

Données en mouvement : HTTPS 256 BITS

Notre standard pour tout le trafic (données en mouvement) dans ou hors de nos serveurs est un **chiffrement systématique par TLS** (protocoles TLS 1.2 et supérieurs) avec les plus hauts niveaux de chiffrement (256 bits). Aucun trafic non chiffré n'est autorisé.

Seuls les navigateurs modernes et sécurisés sont utilisés (Edge, Firefox, Chrome, Safari) ainsi queles applications mobiles natives DiliTrust. L'accès est refusé aux navigateurs obsolètes et non sécurisés (tels que IE8).

Module matériel de sécurité (HSM)

Un « Hardware Security Module » (HSM) est un coffre-fort numérique. C'est un processeur cryptographique dédié, spécialement conçu pour protéger les clés de chiffrement tout au long de leur cycle de vie.

Le HSM agit comme base de confiance protégeant l'infrastructure cryptographique de nos applications en gérant, traitant et conservant de manière sécurisée les clés de chiffrement à l'intérieur d'un serveur à la sécurités spécialement renforcée et **réputée inviolable**. La technologie HSM nous aide à fournir à nos clients le meilleur niveau de chiffrement pour leurs données et le plus haut niveau de sécurité actuellement disponible.

Apportez votre propre clé (BYOK)

Nous offrons à nos clients la possibilité d'héberger eux-mêmes leur propre HSM (**conforme à PKCS11**) pour protéger leur clé de chiffrement. Toutes les données de nos clients seront chiffrées avec leur propre clé. Ces clés sont donc sécurisées dans le HSM client et non au sein du HSM du fournisseur.

Authentification

Mots de passe sécurisés

Chaque utilisateur est identifié par un nom d'utilisateur unique et un mot de passe. Tous les utilisateurs doivent choisir leur propre mot de passe sécurisé. Aucun mot de passe n'est envoyé par courriel ou affiché à aucun moment et à qui que ce soit. Les mots de passe sont enregistrés sous forme de hash, après un cryptage unidirectionnel (injectif).

Chaque mot de passe doit avoir au minimum :

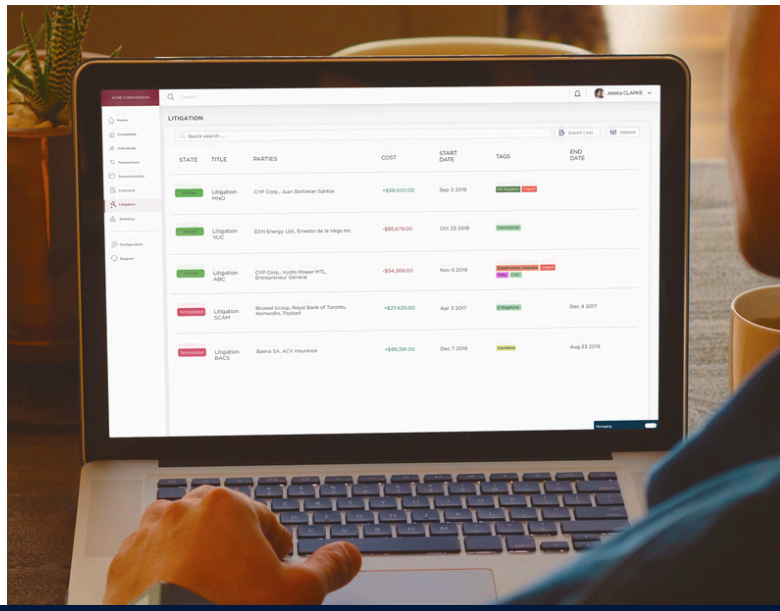
- Trois caractères de différents types (minuscules, majuscules, chiffres ou caractères spéciaux).
- 10 caractères minimum.

Procédure d'obtention ou de récupération de mot de passe : courriel avec lien sécurisé d'accès unique (caduque au bout de 24h et après utilisation).

Chaque requête faite aux serveurs est authentifiée pour vérifier l'identité de l'utilisateur, et si l'utilisateur possède les autorisations appropriées pour exécuter l'action demandée. La demande est transmise pour exécution **si et seulement si tous ces contrôles sont validés avec succès**.

Double authentification par message texte (TFA)

Le TFA (Two Factor Authentication) ou authentification à deux facteurs peut renforcer davantage la sécurité de l'utilisateur pour accéder à l'application. Suite à l'entrée de son identifiant et mot de passe, l'utilisateur **reçoit par message texte** un code à saisir pour finaliser son authentification. Chaque code est à usage unique et correspond à une tentative de connexion spécifique.



Intelligence Artificielle

Une IA 100% propriétaire

Chez DiliTrust, notre approche de l'intelligence artificielle repose sur l'éthique, la responsabilité et la transparence. **Nous concevons et maîtrisons intégralement nos technologies** en interne, ce qui nous permet de garder un contrôle total sur leur conception, leur entraînement et leur fonctionnement sans aucun partage avec un tiers.

Chaque fonctionnalité alimentée par l'IA intègre une supervision humaine, garantissant des résultats fiables et conformes aux attentes métier, en matière de performance comme de sécurité.

Nous sommes résolument engagés à fournir des résultats transparents et explicables. Nos pratiques sont en parfaite adéquation avec le **Règlement européen sur l'IA (AI Act)**, et privilégient l'équité, la responsabilité et la non-discrimination.

Interopérabilité de l'IA

Notre technologie est conçue pour être ouverte et flexible, permettant une intégration fluide avec les modèles de langage étendus (LLM) propres à nos clients.

Grâce à une connectivité **API sécurisée** et à des structures d'IA modulaires, nous offrons aux organisations la possibilité d'exploiter leurs modèles d'IA propriétaire tout en bénéficiant de l'infrastructure sécurisée de DiliTrust.

Chiffré de bout en bout

Chez DiliTrust, la sécurité des données est une priorité absolue. Nous utilisons un chiffrement de bout en bout, avec AES-256 pour les données stockées et TLS 1.2+ pour tous les échanges, garantissant un haut niveau de confidentialité et d'intégrité à chaque étape, qu'il s'agisse d'une analyse contractuelle, d'un résumé de document, ou de tout autre traitement avancé.

Aucune donnée client n'est utilisée pour entraîner des modèles globaux, et tous les traitements IA restent strictement confinés à l'écosystème DiliTrust.

Nos systèmes reposent sur une approche « security-first », en conformité totale avec le RGPD et les normes internationales émergentes. Résultat : une IA éthique, fiable et 100 % maîtrisée.

Protection des données

Nous nous engageons à protéger vos données tout en respectant la réglementation en vigueur, afin de favoriser la confiance et la responsabilité.

- **Réduction des biais** : nos modèles d'IA font l'objet de tests rigoureux et d'une surveillance continue afin d'identifier et de corriger d'éventuels biais, garantissant ainsi des résultats équitables et non discriminatoires.
- **Transparence** : nous avons à cœur de rendre nos processus compréhensibles, en fournissant une documentation claire et des explications précises sur le fonctionnement de nos systèmes et leurs mécanismes de décision.
- **Supervision humaine** : chez DiliTrust, l'IA est conçue pour renforcer la prise de décision humaine, jamais pour la remplacer. Les décisions critiques intègrent systématiquement une validation humaine.

Engagements

Certifiée ISO 27001 & ISO 27701

L'ensemble de la suite DiliTrust est certifiée ISO 27001, la norme internationale de référence pour les systèmes de gestion de la sécurité de l'information (SMSI), garantissant la mise en place de processus rigoureux pour protéger la confidentialité, l'intégrité et la disponibilité des données.

Notre certification ISO 27701 vient renforcer cet engagement en étendant ces exigences à la gestion des informations à caractère personnel, en parfaite conformité avec les réglementations internationales telles que le RGPD.

Ces certifications attestent que notre infrastructure, nos procédures et nos contrôles répondent aux plus hauts standards en matière de sécurité de l'information et de protection des données personnelles.

Respect du SOC 2 type II

DiliTrust est également conforme à la norme SOC 2 Type II, un référentiel d'audit rigoureux élaboré par l'AICPA, qui évalue dans le temps l'efficacité des dispositifs de **protection des données clients** mis en place par un prestataire.

Cette conformité témoigne de notre engagement constant en faveur de la transparence opérationnelle, de la fiabilité de nos systèmes et de la solidité de nos contrôles internes, notamment en matière de sécurité, de disponibilité et de confidentialité.

L'audit SOC 2 offre à nos clients et partenaires la garantie que nos services ne sont pas seulement sécurisés dès la conception, mais font aussi l'objet d'un suivi et d'une amélioration continue face aux risques émergents.

Respect des normes les plus strictes

Notre intelligence artificielle s'inscrit dans un cadre éthique, garantissant l'équité, la transparence et le respect des droits des utilisateurs.

- **Respect du RGPD** : nos systèmes et processus sont conçus pour respecter les normes européennes les plus strictes en matière de protection des données, assurant un traitement des données personnelles licite, équitable et sans aucun partage avec des tiers.
- **La protection de la vie privée dès la conception :** chaque étape du développement et du déploiement de l'IA intègre de solides protections de la vie privée, minimisant les risques et garantissant une conformité réglementaire totale.

Audits

Dans le but d'assurer le plus haut niveau de sécurité, nous appliquons trois niveaux de contrôles redondants : audits internes, audits automatisés hebdomadaires et audits externes humains annuels à minima.

En cas de découverte d'une faille de sécurité, cette dernière est corrigée dans le plus bref délai. Les recommandations et bonnes pratiques sont appliquées systématiquement.

Audits internes

DiliTrust applique des **procédures internes strictes** en termes de sécurité :

- «Sécurité dès la conception» : les équipes de développement sont formées aux différentes techniques d'intrusion et au code sécurisé pour s'en prémunir.
- Procédures internes de revue de code et tests de sécurité avant chaque mise en production de nouvelle fonctionnalité.
- Tests internes de sécurité et utilisation de divers outils d'audit de sécurité, principalement ceux disponibles dans la distribution Linux Kali.

Audits par des experts indépendants

Une fois par an au minimum, nous procédons à un audit de sécurité complet par une entreprise externe indépendante spécialisée dans la sécurité informatique (tests d'intrusion «humains» non automatisés). Un rapport de sécurité est généré à la fin de chaque test; les failles sont corrigées dans le plus bref délai et les recommandations d'amélioration sont appliquées dès que possible.

Audits automatisés

Nos systèmes sont sécurisés par un fournisseur externe. Le service est soumis à un **balayage intensif hebdomadaire** de sécurité niveau serveur (configuration firewall, ports, versions software à jour, configuration SSL... etc.) mais aussi niveau applicatif (XSS, injection SQL, session hijacking... etc.)

"La sécurité est notre ADN"

Nadim Baklouti
CEO, DiliTrust

Pour plus d'informations sur DiliTrust, rendez-vous sur www.dilitrust.com

DiliTrust - 2045 rue Stanley, suite 1500
Montréal, QC H3A 2V4
hello@dilitrust.com

DILITRUST