DiliTrust

Version Deal Evolution

Politique de sécurité

L'infrastructure physique

Les serveurs de DiliTrust sont conformes aux normes de sécurité les plus strictes. Les données hébergées ne sont pas partagées dans le cloud, et ne sont pas soumises à l'US Patriot Act (de quelque manière que ce soit) fournissant ainsi un contrôle permanent sur l'accès à l'information. Les données sont hébergées exclusivement en France.

Hébergement ISO 27001

Afin d'améliorer en permanence la protection des données et garantir la confidentialité de toutes les informations, tous les systèmes et données DiliTrust sont hébergés sur des serveurs qui ont obtenu les plus hautes certifications internationales dans le domaine de la sécurité informatique.

L'hébergement est certifié par la norme internationale ISO / IEC 27001:2013.

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 d'exigences de sécurité.

Sécurité physique

L' accès physique est limité par un système de badge de sécurité, une surveillance vidéo et du personnel de sécurité sur place 24/7.

- Locaux équipés de systèmes de détection de fumée.
- Système de double alimentation systématique.
- Génératrices de secours avec une autonomie initiale de 48 heures.
- Deux connexions réseau (backbone) redondantes.
- A l'intérieur du centre de données, 2 salles de réseaux capables de prendre le relais l'une de l'autre.

Surveillance 24/7

Nos systèmes sont sous surveillance 24/7 pour toute tentative d'attaque ou d'un événement technique :

- Surveillance technique du hardware, taux d'utilisation mémoire, performance applicative…
- Déclenchement automatique d'alertes en cas de détection d'activités suspectes.
- Firewall, IDS (Intrusion Detection System), système anti-flood et protection contre les attaques en force brute.

Sauvegardes (Backups)

Les sauvegardes sont effectuées chaque jour et stockées dans un emplacement secondaire (géographiquement distant) sous les mêmes conditions de sécurité que les serveurs de production.

Les sauvegardes sont conservées pendant un maximum de sept jours (7 jours glissants), puis détruites définitivement sans possibilité de récupération. Exemple : le fichier de sauvegarde du lundi écrase (overwrite) automatiquement le fichier du lundi précédent.

DiliTrust

Version Deal Evolution

Politique de sécurité

Chiffrement

« Data-at-rest »: AES 256

Toutes les données confidentielles au repos sont chiffrées en utilisant le standard de chiffrement avancé : AES (Advanced Encryption Standard, Rijndael) avec une clé de 256 bits. À la fois sur les serveurs et sur les appareils mobiles (pour les données stockées localement).

« Data-in-motion »: 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 1.0, 1.1 et 1.2 seulement) avec les plus hauts niveaux de chiffrement (256 bits). Aucun trafic non chiffré n'est autorisé. Seuls les navigateurs modernes et sécurisés sont autorisés (IE9+, Firefox, Chrome, Safari) et les applications mobiles natives DiliTrust. L'accès est refusé avec les navigateurs obsolètes et non sécurisés (tels que IE6).

Niveau applicatif

2 niveaux de contrôles de sécurité redondants : audits internes et audits externes humains périodiques. En cas de découverte d'une faille de sécurité, elle est corrigée dans le plus bref délai. Les recommandations et bonnes pratiques sont appliquées systématiquement.

Audits internes

DiliTrust applique des procédures internes strictes pour faire appliquer les meilleures pratiques de sécurité :
• Procédures internes de « revue de code » et tests de sécurité avant chaque mise en production de nouvelle fonctionnalité.
• Tests internes de sécurité et utilisation d'outils d'audit de sécurité. Principalement ceux disponibles dans la distribution Linux Kali (sqlmap, burpsuite, nmap etc).

Audits externes par des experts indépendants

Une à deux fois par an minimum, nous procédons à un audit de sécurité complet par une entreprise externe spécialisée dans la sécurité informatique (tests d'intrusion « humains » non-automatisés).

Politique de mot de passe

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 mail 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).

La politique de mot de passe minimum par défaut est la suivante :
• Contenir au moins trois caractères de différents types (minuscules, majuscules, chiffres ou de ponctuation).
• Avoir une longueur minimum de 10 caractères.

Procédure de récupération de mot de passe (ou premier accès) : mail avec lien sécurisé d'accès unique (caduque au bout de 24h et après utilisation). Chaque demande faite à nos 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 ces contrôles sont validés avec succès.

Option d'authentification forte par SMS (TFA = Two factor authentication) : suite à l'entrée de son login et mot de passe, l'utilisateur reçoit un SMS avec un troisième code à rentrer pour finaliser son authentification. Chaque code est à usage unique et correspond à une tentative de connexion spécifique.