

PRÉSENTATI ON DE LA SÉCURITÉ DE FOXIT ESIGN



LIVRE BLANC

TABLE DES MATIÈRES

Sécurité dynamique et chiffrement	3
Visibilité	5
Audit	5
Centres de données	5
Maintien de l'activité/Récupération d'urgence	6
Politique de conservation des données	7



La sécurité est au cœur de Foxit eSign. Comme c'est le cas pour tous nos produits, Foxit eSign a été développé et conçu en ayant la sécurité en tête.

Ce document donne un aperçu des technologies, stratégies et pratiques de sécurité utilisées par Foxit eSign qui permettent de protéger vos documents et vos données, en incluant les informations qui vous permettent d'effectuer des configurations de sécurité pour répondre aux exigences uniques en matière de gestion des risques et de conformité de votre entreprise.

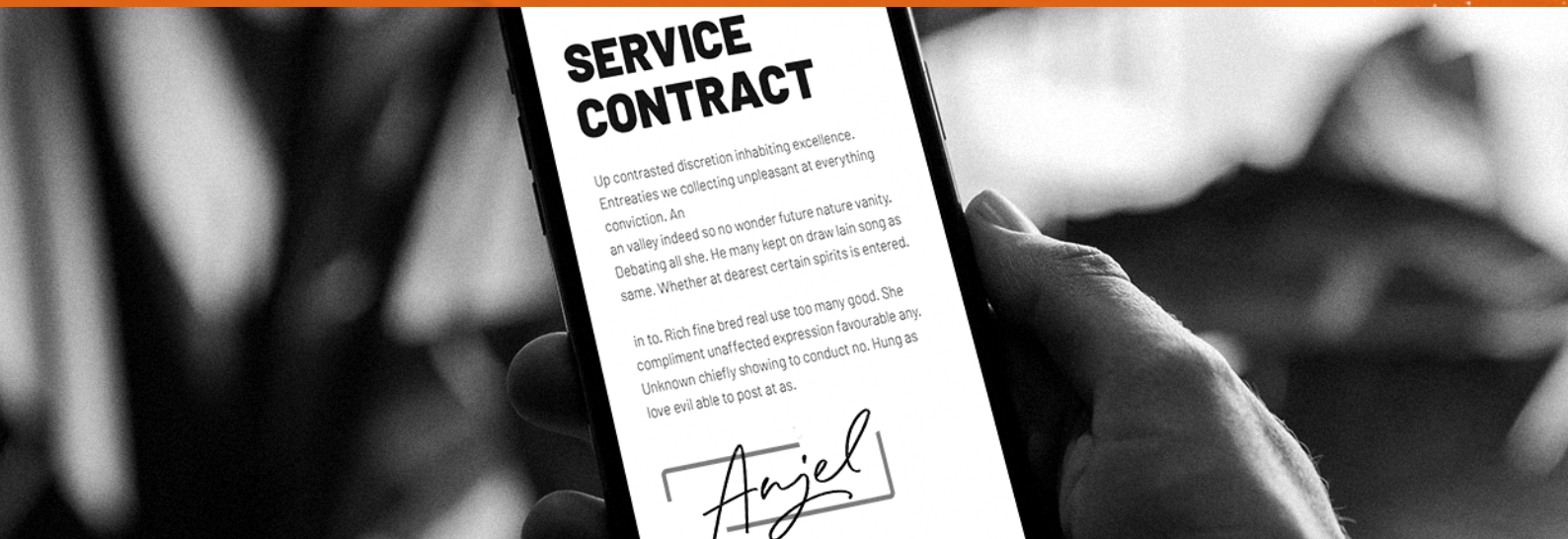
Ce document répertorie également plusieurs réglementations régionales auxquelles Foxit eSign se conforme strictement afin de vous assurer d'être en mesure de procéder au déploiement.

SÉCURITÉ DYNAMIQUE ET CHIFFREMENT

Foxit eSign est certifié SOC 2 Type 2. Il est régulièrement contrôlé par des auditeurs indépendants du secteur afin de garantir une conformité rigoureuse avec les 5 principes du service de confiance. Les éléments suivants décrivent les grandes lignes des engagements de service que Foxit eSign effectue envers les entités utilisatrices, les lois et réglementations qui régissent les dispositions de sa signature électronique et les services de gestion de la productivité, ainsi que les exigences relatives à la finance, à l'exploitation et à la conformité que Foxit eSign a établies pour ses services.

Sécurité : protection de vos données contre tout accès ou affichage non autorisé dans notre système

- Foxit eSign s'engage à utiliser des mesures administratives et techniques conformes aux pratiques applicables de l'industrie afin de protéger le système et empêcher la perte accidentelle ou l'accès non autorisé, l'utilisation, la modification ou la divulgation des données des clients qui sont sous son contrôle pendant chaque période de commande.
- Toutes les données transmises entre nos systèmes et les utilisateurs sont protégées à l'aide des protocoles TLS (Transport Layer Security) et HSTS (HTTP Strict Transport Security).
- L'accès aux environnements qui contiennent des données clients nécessite une série de contrôles d'authentification et d'autorisation, notamment l'authentification MFA (Multi-Factor Authentication).



Disponibilité : garantie que notre logiciel est disponible comme souhaité et convenu

- Foxit eSign s'engage à effectuer des efforts raisonnables sur le plan commercial pour rendre l'accès et l'utilisation du système disponibles aux utilisateurs finaux via Internet au moins 99,95 % du temps (mesuré au cours de chaque mois calendaire), en excluant l'indisponibilité due à la maintenance programmée. Toutefois, Foxit eSign a conservé une disponibilité de plus de 99,99 % au cours des 5 dernières années.

Confidentialité : conservation de vos données protégées, privées et confidentielles

- Foxit eSign s'engage à protéger les informations confidentielles contre toute utilisation ou divulgation non autorisée dans la même mesure qu'il protège ses propres informations confidentielles. En aucun cas, nous n'utiliserons une norme inférieure à ce qui est raisonnable pour protéger de telles informations confidentielles.
- Nous utilisons les informations confidentielles uniquement aux fins pour lesquelles elles ont été divulguées.

Intégrité du traitement : tout le traitement du système s'effectue comme autorisé, de manière précise et rapide

- La configuration système et les pratiques de Foxit eSign incluent des contrôles de surveillance des performances de l'API (Application Programming Interface), la surveillance des arrivées de données, et le respect des stratégies et procédures qui contribuent à la prévention, la détection et la correction des erreurs de traitement des données.

Confidentialité : respect rigoureux des principes généralement reconnus en matière de confidentialité (GAPP, Generally Accepted Privacy Principles), qui régissent la conservation, la collecte, l'utilisation, la divulgation et la destruction de toutes les données personnelles comme prévu dans notre Avis de confidentialité

- Foxit eSign s'engage à protéger les informations personnelles identifiables contre toute utilisation ou divulgation non autorisée dans la même mesure qu'il protège ses propres informations personnelles identifiables. En aucun cas, nous n'utiliserons une norme inférieure à ce qui est raisonnable pour protéger de telles informations personnelles identifiables.
- Nous utilisons les informations personnelles identifiables uniquement aux fins pour lesquelles elles ont été divulguées.

En outre, vos documents sont verrouillés et sécurisés par un chiffrement sur 256 bits de qualité industrielle et associés à des contrôles de pare-feu stricts : tout le trafic entrant et sortant est surveillé et contraint de se conformer aux règles de sécurité de notre réseau. Foxit eSign fournit une protection de bout en bout en chiffrant les données au repos et en mouvement.



VISIBILITÉ

Foxit eSign offre aux clients des contrôles de visibilité complète afin qu'ils puissent décider quelles sont les personnes qui peuvent voir les documents de leur entreprise et y accéder. Cela inclut les contrôles suivants :

- Personnalisez les fonctionnalités de visibilité afin de limiter l'affichage des documents aux seuls destinataires désignés que vous choisissez.
- Restreignez la visibilité de l'utilisateur du compte avec des fonctionnalités telles que l'Accès aux champs sécurisé, qui accorde l'accès aux informations des champs sécurisés uniquement aux utilisateurs approuvés.
- Contrôlez l'accès aux informations en concevant différents niveaux et partages pour les utilisateurs.
- Attribuez des responsables aux utilisateurs et administrateurs réguliers, ce qui facilite la surveillance et l'utilisation des documents qui leur sont associés.

AUDIT

Le fait de savoir exactement où se trouvent vos documents et où ils ont été est un élément essentiel de la sécurité et de la conformité. Foxit eSign fournit des rapports et des fonctionnalités d'audit détaillés afin que les clients puissent rester informés des flux de travail de leurs documents.

- Des pistes d'audit détaillées suivent chaque document en fonction de l'adresse IP et de l'horodatage, de sorte que vous disposez en permanence d'une connaissance complète du lieu, du moment et des personnes qui consultent vos documents.
- Certificat d'achèvement fourni pour chaque document, avec l'adresse IP, l'adresse e-mail, l'horodatage et le nom du signataire qui lui sont associés.
- Suivez la suppression des documents et des dossiers à chaque étape du processus. Notre historique de suppression des dossiers vous permet de voir où, quand et par qui le dossier a été supprimé.

CENTRES DE DONNÉES

Il est important que nos clients comprennent où sont stockés leurs documents. Nous comprenons également l'importance de la résidence locale des données pour nos clients. À cet effet, Foxit eSign utilise les centres de données d'AWS (Amazon Web Services). Nos centres de données sont conçus pour anticiper et tolérer des pannes, tout en maintenant les niveaux de service, et l'accès au centre de données est contrôlé régulièrement.

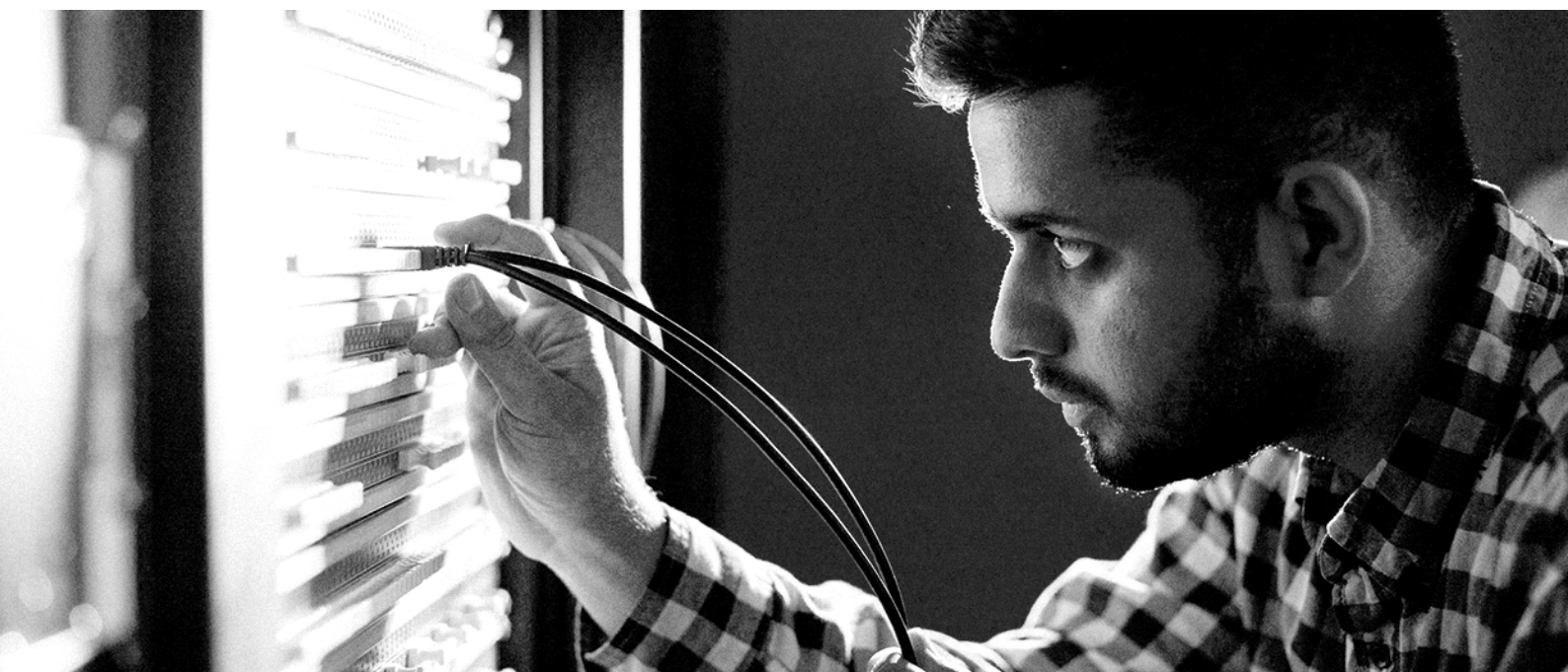
Emplacement des données : Foxit eSign maintient des centres de données approuvés aux États-Unis et en Europe avec des installations SSAE16 conformes aux normes SOC 2 Type 2 et PCI. Aux États-Unis, les applications sont hébergées sur la plateforme AWS et fonctionnent principalement dans des locaux situés en Virginie du Nord (Est des États-Unis), dans l'Ohio (Est des États-Unis) et dans le nord de la Californie (Ouest des États-Unis). En Europe, les centres de données se trouvent à Francfort, en Allemagne. Au Canada, les centres de données se trouvent à Montréal. Ces installations sont verrouillées et surveillées 24 heures sur 24 pour garantir que vos données sont stockées uniquement sur les serveurs les plus sûrs et les plus sécurisés.

Résidence des données : lors de l'inscription à un compte Foxit eSign, votre compte sera affecté à votre région locale pour le stockage serveur. Nous proposons également à nos clients la possibilité de choisir dans quel centre de données ils souhaitent stocker leurs documents. Finalement, les clients disposent d'un contrôle total pour définir qui accède à leurs documents.

MAINTIEN DE L'ACTIVITÉ/RÉCUPÉRATION D'URGENCE

Les données et les fichiers de Foxit eSign sont stockés sur des serveurs et des bases de données gérées à haute disponibilité, et sont également synchronisés en temps réel avec les bases de données et les serveurs chiffrés pour les rapports et la sauvegarde. En cas d'urgence, les systèmes peuvent être mis en ligne à partir de la sauvegarde ou d'une autre zone de disponibilité.

En outre, Foxit eSign maintient une capacité de système robuste et une surveillance de l'infrastructure pour assurer les performances et la disponibilité. Les sauvegardes sont effectuées quasiment en temps réel et sont essentiellement un processus continu. La planification de la continuité de l'activité et de la récupération d'urgence chez Foxit eSign prend en compte une analyse des conséquences sur l'activité (BIA, Business Impact Analysis), la gestion des incidents, les événements imprévus et les plans de continuité de l'activité, qui constituent collectivement le cadre du maintien de la stratégie de continuité et d'urgence, de la gestion et des plans opérationnels. Foxit eSign a conçu des stratégies et des procédures qui couvrent une panne partielle ou complète des fournisseurs de services cloud (CSP, Cloud Service Providers).





POLITIQUE DE CONSERVATION DES DONNÉES

Notre politique de conservation des données décrit les directives importantes indiquant pendant combien de temps nous suivons et conservons vos informations, et à quel moment elles sont éliminées. Les politiques de conservation varient selon le type de compte. Les politiques de type de compte sont définies comme suit :

Comptes d'essai : les documents et les données qui sont associées à des comptes non payants seront supprimés au bout de 30 jours, sauf si le compte est converti en compte payant par l'utilisateur.

Comptes payants : les ébauches de documents de comptes payants seront stockées dans le système pendant 45 jours, sauf si les documents sont envoyés pour signature. Les utilisateurs de comptes payants peuvent également configurer leur propre politique de conservation des documents pour chaque type de document, y compris les documents partagés, partiellement signés, exécutés, annulés et/ou expirés.