VISÃO GERAL DE SEGURANÇA DO FOXIT ESIGN

WHITEPAPER

SUMÁRIO

A segurança é o núcleo fundamental do Foxit eSign. Como acontece com todos os nossos produtos, o Foxit eSign foi desenvolvido e projetado pensando na segurança.

Este documento oferece uma visão geral das tecnologias, políticas e práticas de segurança usadas pelo Foxit eSign que protegem seus documentos e dados, incluindo informações que permitem que você faça configurações de segurança para atender aos requisitos de conformidade e gerenciamento de riscos exclusivos da sua empresa.

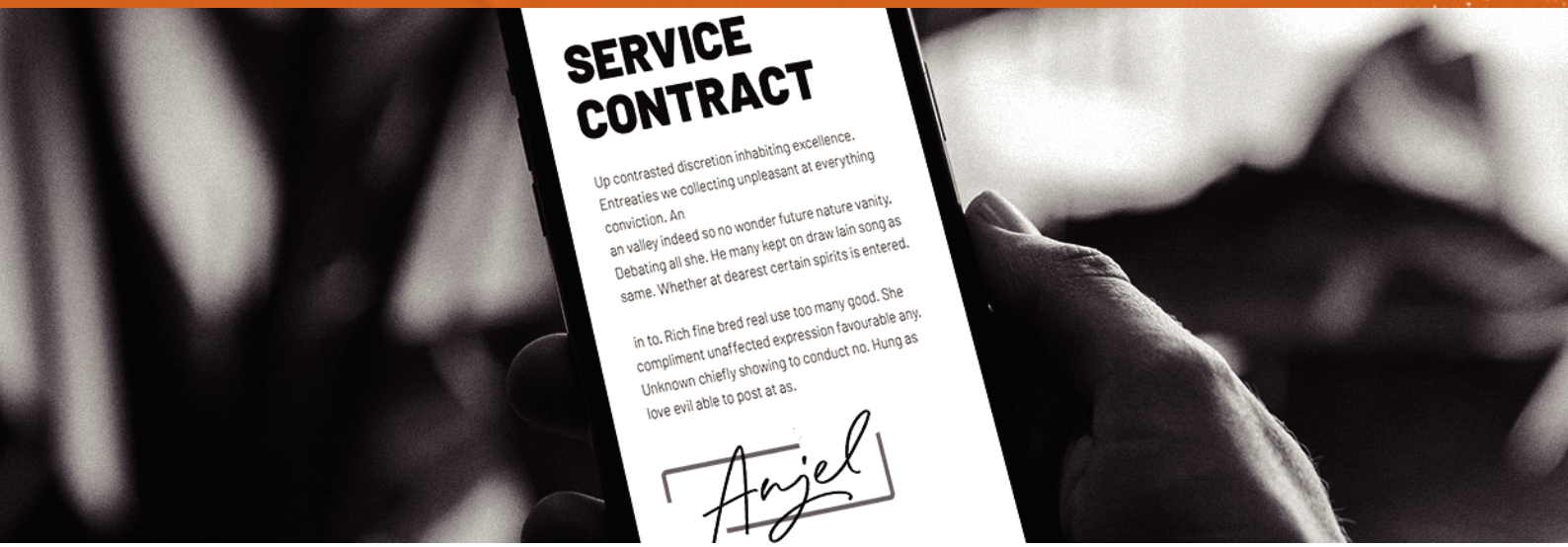
Este documento também identifica vários regulamentos regionais que o Foxit eSign cumpre de forma estrita para garantir que você seja capaz de implantar.

SEGURANÇA E CRIPTOGRAFIA DINÂMICAS

O Foxit eSign é certificado pelo SOC 2 Tipo 2. Ele é regularmente auditado por auditores independentes do setor para garantir a conformidade estrita com os 5 Princípios de serviço de confiança. O seguinte descreve os compromissos de serviço que o Foxit eSign estabelece com as entidades usuárias, as leis e regulamentos que regem o fornecimento de seus serviços de gerenciamento de produtividade e assinatura eletrônica e os requisitos financeiros, operacionais e de conformidade que o Foxit eSign estabeleceu para seus serviços.

Segurança – Proteção dos seus dados contra acesso não autorizado e visualização por meio do nosso sistema

- O Foxit eSign se compromete a empregar medidas administrativas e técnicas de acordo com as práticas aplicáveis do setor para proteger o sistema e evitar a perda acidental ou o acesso não autorizado, o uso, a alteração ou a divulgação de dados do cliente sob seu controle durante o prazo de cada pedido.
- Todos os dados transmitidos entre nossos sistemas e usuários são protegidos por segurança da camada de transporte (TLS) e segurança de transporte estrito HTTP (HSTS).
- O acesso a ambientes que contêm dados do cliente requer uma série de controles de autenticação e autorização, incluindo autenticação multifator (MFA).



Disponibilidade - Garantir que nosso software esteja disponível conforme necessário e acordado

- O Foxit eSign se compromete a empenhar esforços comercialmente razoáveis para disponibilizar o sistema para acesso e uso por usuários finais na Internet pelo menos 99,95% do tempo, conforme medido ao longo de cada mês, excluindo indisponibilidade como resultado de manutenção programada. No entanto, o Foxit eSign manteve um tempo de atividade de mais de 99,99% nos últimos 5 anos.

Confidencialidade – Manter seus dados protegidos, privados e confidenciais

- O Foxit eSign se compromete a proteger as informações confidenciais contra qualquer uso ou divulgação não autorizada, na mesma medida em que protegemos nossas próprias informações confidenciais. Em nenhum caso, usaremos menos do que um padrão razoável de cuidado para proteger essas informações confidenciais.
- Usamos as informações confidenciais apenas para os fins para os quais foram divulgadas.

Integridade de processamento – Todo o processamento do sistema é concluído conforme autorizado, preciso e imediato

- Os requisitos e práticas do sistema do Foxit eSign incluem controles de monitoramento de desempenho da interface de programação de aplicativos (API), monitoramento de entradas de dados e manutenção de políticas e procedimentos que auxiliam na prevenção, detecção e correção de erros de processamento de dados.

Privacidade – Cumprimento estrito dos Princípios de Privacidade Geralmente Aceitos (GAPP, Generally Accepted Privacy Principles), que determina que todas as informações pessoais sejam retidas, coletadas, usadas, divulgadas e destruídas conforme estabelecido em nosso aviso de privacidade

- O Foxit eSign se compromete a proteger as informações de identificação pessoal contra qualquer uso ou divulgação não autorizada, na mesma medida em que protegemos nossas próprias informações de identificação pessoal. Em nenhum caso, usaremos menos do que um padrão razoável de cuidado para proteger tais informações pessoalmente identificáveis.
- Usamos informações de identificação pessoal unicamente para os fins para os quais foram divulgadas.

Além disso, seus documentos são bloqueados e protegidos com criptografia de 256 bits de nível industrial e emparelhados com controles de firewall rígidos – todo o tráfego de entrada e saída é monitorado e forçado a obedecer as rígidas regras de segurança da nossa rede. O Foxit eSign fornece proteção de ponta a ponta, criptografando os dados em repouso e em movimento.

VISIBILIDADE

O Foxit eSign oferece aos clientes controles de visibilidade total para que você possa decidir quem pode ver e acessar os documentos da sua organização. Isso inclui os seguintes controles:

- Recursos de visibilidade personalizados para limitar a visualização do documento apenas aos destinatários designados que você escolher.
- Restrição da visibilidade do usuário da conta com recursos como Acesso a Campo Seguro, que fornece acesso apenas de usuários aprovados às informações em campos seguros.
- Controle do acesso às informações designando diferentes níveis de usuário e configurações de compartilhamento.
- Atribuição de gerentes a usuários e administradores regulares, garantindo fácil monitoramento e uso de documentos subordinados.

AUDITORIA

Saber exatamente onde seus documentos estão e onde estiveram é um componente crucial de segurança e conformidade. O Foxit eSign fornece relatórios e recursos de auditoria detalhados para que os clientes possam se manter informados sobre seus fluxos de trabalho de documentos.

- Trilhas de auditoria detalhadas rastreiam cada documento por endereço IP e carimbo de data/hora, para que você tenha sempre total conhecimento de onde, quando e quem está visualizando seus documentos.
- Certificado de conclusão fornecido para cada documento com endereço IP, endereço de e-mail, carimbo de data/hora e nome do signatário associados.
- Acompanhe a exclusão de documentos e pastas em cada etapa do processo. Nosso histórico de exclusão de pastas permite que você veja onde, quando e por quem cada pasta foi excluída.

DATA CENTERS

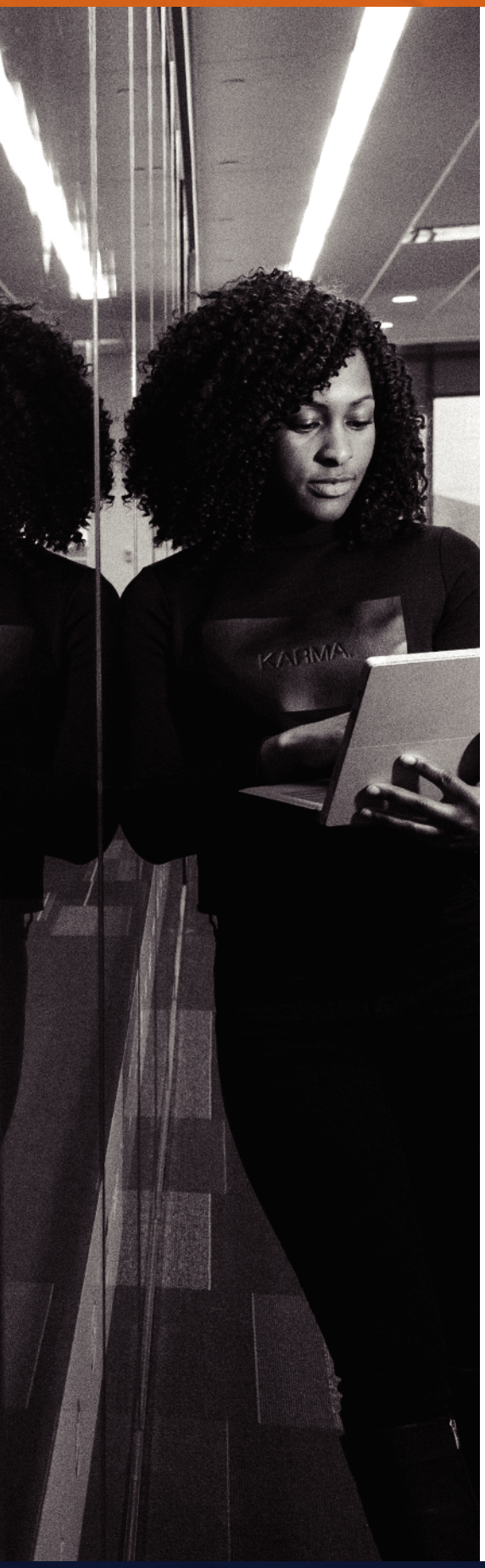
É importante que nossos clientes entendam onde seus documentos estão sendo armazenados. Também entendemos a importância da residência de dados local para nossos clientes. Para isso, o Foxit eSign usa data centers da Amazon Web Services (AWS). Nossos data centers são projetados para antecipar e tolerar falhas enquanto mantêm os níveis de serviço, e o acesso aos data centers é revisado regularmente.

Localização de dados – O Foxit eSign mantém os data centers confiáveis nos EUA e na Europa com instalações SSAE16 que estão em conformidade com o SOC 2 Tipo 2 e o PCI. Nos Estados Unidos, os aplicativos são hospedados na plataforma AWS e operam principalmente em instalações localizadas no Norte da Virgínia (Leste dos EUA), Ohio (Leste dos EUA) e Norte da Califórnia (Oeste dos EUA). Na Europa, os data centers estão localizados em Frankfurt, na Alemanha. No Canadá, os data centers estão localizados em Montreal. Essas instalações são bloqueadas e monitoradas 24 horas por dia para garantir que seus dados sejam armazenados apenas nos servidores mais seguros e protegidos.

Residência de dados – Ao inscrever-se em uma conta do Foxit eSign, sua conta será atribuída à sua região local para armazenamento do servidor. Também oferecemos aos nossos clientes a opção de escolher em qual data center eles gostariam de armazenar seus documentos. Por fim, os clientes têm controle total sobre quem acessa seus documentos.

CONTINUIDADE DE NEGÓCIOS/RECUPERAÇÃO DE DESASTRES

Os dados e arquivos do Foxit eSign são armazenados em servidores de alta disponibilidade e bancos de dados gerenciados, e também são sincronizados em tempo real com os bancos de dados e servidores de arquivos criptografados de relatório e backup. Em caso de emergência, os sistemas podem ser colocados online pelo backup ou por outra zona de disponibilidade.



Além disso, o Foxit eSign mantém a capacidade robusta do sistema e o monitoramento da infraestrutura para desempenho e disponibilidade. Os backups são executados quase em tempo real e são, em grande parte, um processo contínuo. O planejamento de continuidade de negócios e recuperação de desastres no Foxit eSign leva em consideração uma Análise de impacto nos negócios (BIA), tratamento de incidentes, planos de contingência e continuidade de negócios que, coletivamente, constituem a estrutura para manter uma estratégia de continuidade e contingência, planos de gerenciamento e operacionais. O Foxit eSign projetou políticas e procedimentos que cobrem uma falha parcial ou total dos provedores de serviços em nuvem (CSPs).

POLÍTICA DE RETENÇÃO DE DADOS

Nossa política de retenção de dados descreve diretrizes importantes sobre por quanto tempo rastreamos e mantemos suas informações e quando elas são descartadas. As políticas de retenção variam de acordo com o tipo de conta. As políticas de tipo de conta são definidas da seguinte forma:

Contas de avaliação – Documentos de contas não pagas e dados relacionados serão excluídos após 30 dias, a menos que a conta seja convertida em uma conta paga pelo usuário.

Contas pagas – Os documentos de saque de conta paga serão armazenados no sistema por 45 dias, a menos que os documentos sejam enviados para assinatura. Os usuários de contas pagas também podem configurar suas próprias políticas de retenção de documentos para cada tipo de documento, incluindo documentos compartilhados, parcialmente assinados, executados, cancelados e/ou expirados.