



FOXIT ESIGN - PANORAMICA SULLA SICUREZZA



WHITEPAPER

SOMMARIO

Sicurezza dinamica e crittografia	3
Visibilità	5
Auditing	5
Data center	5
Continuità aziendale/Ripristino di emergenza	6
Criteri di conservazione dei dati	7



La sicurezza costituisce il nucleo di Foxit eSign. Come nel caso di tutti i nostri prodotti, Foxit eSign è stato sviluppato e progettato mettendo la sicurezza al primo posto.

Questo documento fornisce una panoramica delle tecnologie di sicurezza, le prassi e i criteri utilizzati da Foxit eSign per proteggere documenti e dati, comprese le informazioni che permettono di realizzare configurazioni di sicurezza per soddisfare i requisiti specifici di gestione del rischio e di conformità dell'azienda.

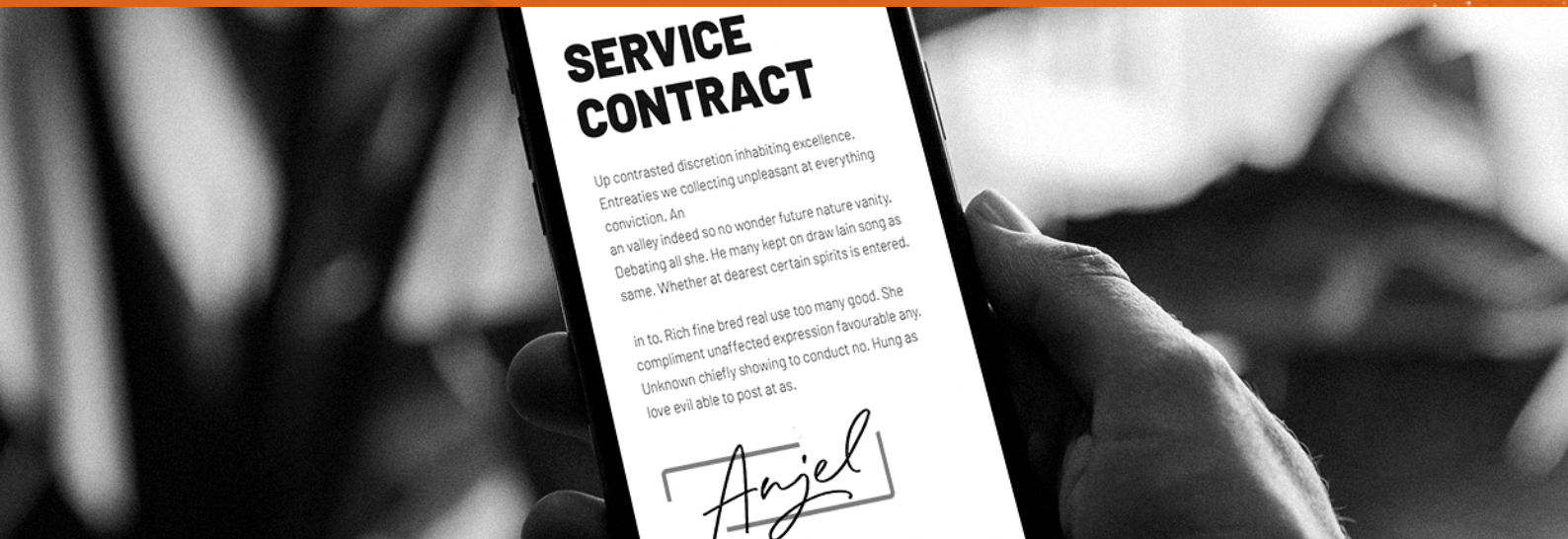
Questo documento indica anche diversi regolamenti locali che Foxit eSign rispetta rigorosamente per garantire la possibilità di implementazione.

SICUREZZA DINAMICA E CRITTOGRAFIA

Foxit eSign è certificato SOC 2 Type 2. È regolarmente controllato da auditor indipendenti del settore per garantire la stretta osservanza dei 5 Trust Service Principles. Quanto segue delinea gli impegni di servizio che Foxit eSign si assume nei confronti di utenti, leggi e normative che regolano la fornitura dei suoi servizi di firma elettronica e di gestione della produttività, e i requisiti finanziari, operativi e di conformità che Foxit eSign ha stabilito per i suoi servizi.

Sicurezza - Protezione dei dati da accessi e visualizzazioni non autorizzate attraverso il nostro sistema

- Foxit eSign è impegnata nell'uso di misure amministrative e tecniche conformi con le pratiche del settore applicabili per proteggere il sistema e prevenire la perdita accidentale o l'accesso non autorizzato, l'uso, l'alterazione o la divulgazione dei dati del cliente sotto il suo controllo per tutta la durata dell'ordine.
- Tutti i dati trasmessi tra i nostri sistemi e gli utenti sono protetti utilizzando Transport Layer Security (TLS) e HTTP Strict Transport Security (HSTS).
- L'accesso agli ambienti che contengono i dati dei clienti richiede una serie di controlli di autenticazione e autorizzazione, compresa l'autenticazione a più fattori (MFA).



Disponibilità - Assicurazione della disponibilità del nostro software come necessario e concordato

- Foxit eSign si impegna a compiere sforzi economicamente ragionevoli per rendere il sistema disponibile per l'accesso e l'uso da parte degli utenti finali su Internet almeno per il 99,95% di ogni mese di calendario, escludendo l'indisponibilità a seguito di manutenzione programmata. Tuttavia, Foxit eSign ha mantenuto un uptime di oltre il 99,99% negli ultimi 5 anni.

Riservatezza - Mantenimento della protezione, sicurezza e riservatezza dei dati

- Foxit eSign si impegna a proteggere le informazioni riservate da qualsiasi uso o divulgazione non autorizzata nella stessa misura in cui protegge le proprie informazioni riservate. In nessun caso adotteremo uno standard di protezione meno che ragionevole per proteggere tali informazioni riservate.
- Utilizziamo le informazioni riservate esclusivamente per lo scopo per il quale sono state divulgate.

Integrità dell'elaborazione - Tutta l'elaborazione del sistema è autorizzata, accurata e tempestiva

- I requisiti e le pratiche di sistema di Foxit eSign includono i controlli di monitoraggio delle prestazioni dell'interfaccia di programmazione dell'applicazione (API), il monitoraggio degli ingressi dei dati e il mantenimento di criteri e procedure che aiutano a prevenire, rilevare e correggere gli errori di elaborazione dei dati.

Privacy - Adesione rigorosa ai principi di privacy generalmente accettati (GAPP, Generally Accepted Privacy Principles) che impongono che tutte le informazioni personali siano conservate, raccolte, utilizzate, divulgate e distrutte come stabilito nella nostra informativa sulla privacy

- Foxit eSign si impegna a proteggere le informazioni che consentono l'identificazione da qualsiasi uso o divulgazione non autorizzata nella stessa misura in cui proteggiamo le nostre informazioni che consentono l'identificazione. In nessun caso adotteremo uno standard di protezione meno che ragionevole per proteggere tali informazioni che consentono l'identificazione.
- Utilizziamo le informazioni personali che consentono l'identificazione esclusivamente per lo scopo per il quale sono state divulgate

Inoltre, i documenti sono bloccati e protetti con una crittografia a 256 bit di livello industriale e protetti tramite severi controlli del firewall: tutto il traffico in entrata e in uscita è monitorato e costretto a rispettare le severe regole di sicurezza della nostra rete. Foxit eSign fornisce una protezione end-to-end criptando i dati inattivi e in movimento.



VISIBILITÀ

Foxit eSign offre ai clienti controlli di visibilità completa in modo da poter decidere chi può vedere e accedere ai documenti dell'organizzazione. Questo include i seguenti controlli:

- Personalizzazione delle caratteristiche di visibilità per limitare la visualizzazione dei documenti solo ai destinatari designati che hai scelto.
- Limitazione della visibilità dell'utente dell'account con funzioni come Secured Field Access, che dà solo agli utenti approvati l'accesso alle informazioni nei campi protetti.
- Controllo dell'accesso alle informazioni indicando livelli differenti di utenti e impostazioni di condivisione.
- Assegnazione di responsabili agli utenti regolari e agli amministratori, assicurando un facile monitoraggio e il conseguente uso dei documenti.

AUDITING

Sapere esattamente dove sono e dove sono stati i documenti è una componente cruciale della sicurezza e della conformità. Foxit eSign fornisce report e funzioni di controllo dettagliati in modo che i clienti possano rimanere informati sui flussi di lavoro documentali.

- Gli audit trail dettagliati tracciano ogni documento in base a indirizzo IP e timestamp, così avrai la possibilità di sapere sempre in modo dettagliato la posizione, il momento e il nome di chi stia visualizzando i documenti.
- Certificato di completamento fornito per ogni documento con l'indirizzo IP associato, indirizzo e-mail, timestamp e nome del firmatario.
- Monitora la cancellazione di documenti e cartelle in ogni fase. La nostra cronologia di eliminazione delle cartelle ti permette di vedere dove, quando e da chi è stata eliminata qualsiasi cartella.

DATA CENTER

È importante che i nostri clienti capiscano dove vengono conservati i loro documenti. Comprendiamo anche l'importanza della permanenza locale dei dati per i nostri clienti. A tal fine, Foxit eSign utilizza data center Amazon Web Services (AWS). I nostri data center sono progettati per anticipare e tollerare i guasti, garantendo i livelli di servizio, mentre l'accesso ai data center viene regolarmente verificato.

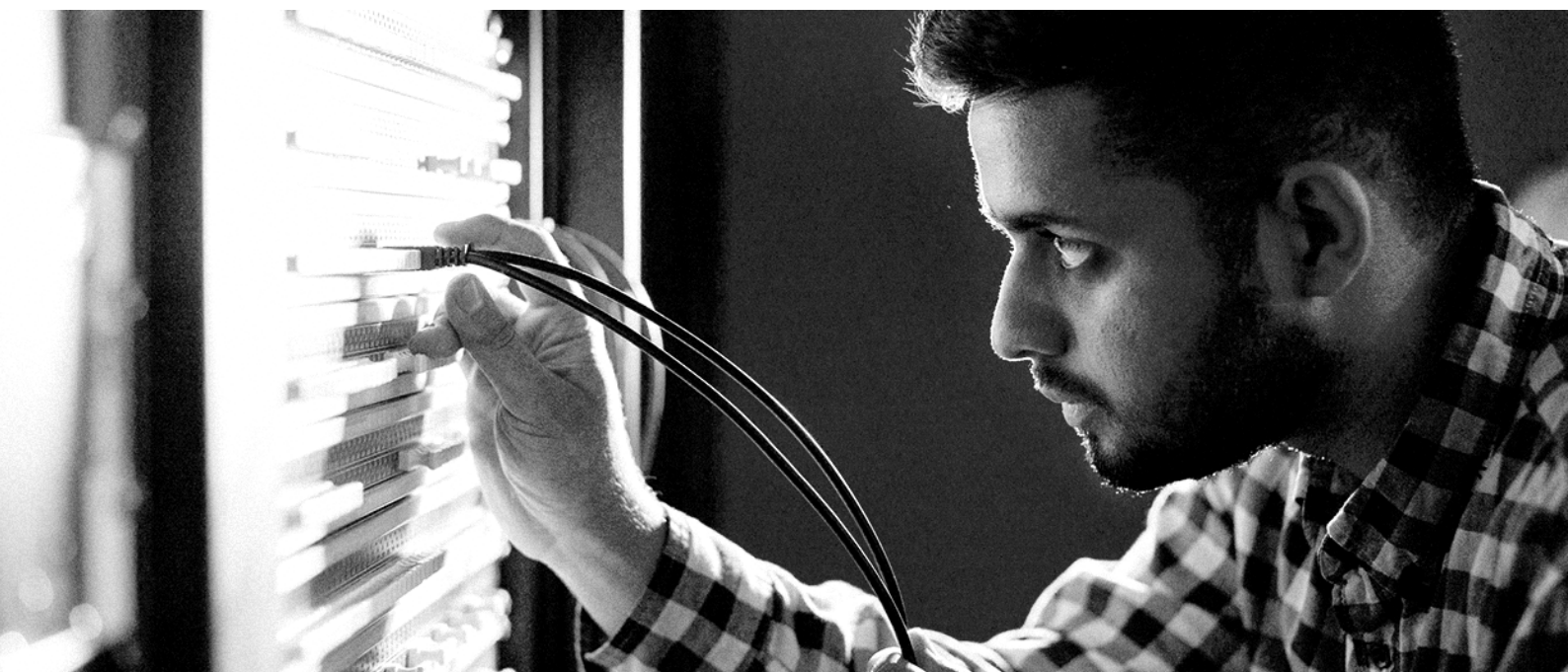
Ubicazione dei dati - Foxit eSign mantiene data center affidabili negli Stati Uniti e in Europa con strutture SSAE16 conformi a SOC 2 Type 2 e a PCI. Negli Stati Uniti, le applicazioni sono ospitate sulla piattaforma AWS e operano principalmente in strutture situate in Virginia del Nord (USA orientali), Ohio (USA orientali) e Nord California (USA occidentali). In Europa, i data center si trovano a Francoforte, in Germania. In Canada, i data center si trovano a Montreal. Queste strutture sono chiuse e monitorate 24 ore su 24 per garantire che i dati siano memorizzati solo sui server più sicuri e protetti.

Residenza dei dati - Quando ti iscrivi per ottenere un account Foxit eSign, l'account sarà assegnato alla tua regione per l'archiviazione sul server. Forniamo anche ai nostri clienti la possibilità di scegliere in quale data center desiderano conservare i loro documenti. Infine, i clienti hanno il pieno controllo su chi accede ai loro documenti.

CONTINUITÀ AZIENDALE/RIPRISTINO DI EMERGENZA

I dati e i file di Foxit eSign sono memorizzati in server ad alta disponibilità e database gestiti e sono anche sincronizzati in tempo reale con i database e i server di file criptati di reporting e backup. In caso di emergenza, i sistemi possono essere portati online dal backup o da un'altra zona di disponibilità.

Inoltre, Foxit eSign offre una solida capacità di sistema e il monitoraggio dell'infrastruttura per le prestazioni e la disponibilità. I backup vengono eseguiti quasi in tempo reale e sono in gran parte un processo continuo. La pianificazione della continuità aziendale e del ripristino di emergenza di Foxit eSign prende in considerazione una Business Impact Analysis (BIA), la gestione degli incidenti, la contingenza e i piani di continuità aziendale, che collettivamente costituiscono il contesto per mantenere una strategia di continuità e di contingenza, la gestione e i piani operativi. Foxit eSign ha ideato prassi e procedure che coprono un malfunzionamento parziale o completo dei fornitori di servizi cloud (CSP).





CRITERI DI CONSERVAZIONE DEI DATI

I nostri criteri di conservazione dei dati delineano importanti linee guida sul tempo per il quale monitoriamo e conserviamo le informazioni, e quando queste vengono eliminate. I criteri di conservazione differiscono in base al tipo di account. I criteri relativi ai tipi di account sono definiti come segue:

Account di prova - I documenti degli account non a pagamento e i relativi dati saranno cancellati dopo 30 giorni, a meno che l'account non venga convertito in un account a pagamento dall'utente.

Account a pagamento - I documenti degli account a pagamento saranno conservati nel sistema per 45 giorni, a meno che i documenti non vengano inviati per la firma. Gli utenti degli account a pagamento possono anche configurare i propri criteri di conservazione dei documenti per ogni tipo di documento, compresi i documenti condivisi, parzialmente firmati, eseguiti, annullati e/o scaduti.