

A black and white photograph of a man with a beard and short hair, wearing a suit jacket over a striped shirt. He is looking down at a smartphone he is holding in his hands. The background is a blurred office or cityscape view from a window.

OVERZICHT VAN BEVEILIGINGS- FUNCTIES FOXIT ESIGN

INHOUDSOPGAVE

Dynamische beveiliging en versleuteling	3
Zichtbaarheid	5
Controle	5
Datacentra	5
Bedrijfscontinuïteit/Herstel na noodgeval	6
Beleid inzake gegevensbewaring	7



Veiligheid is de fundamentele kern van Foxit eSign. Zoals al onze producten is Foxit eSign ontwikkeld en ontworpen met beveiliging als prioriteit.

Dit document bevat een overzicht van de beveiligingstechnologieën, -beleidslijnen en -praktijken die Foxit eSign gebruikt om uw documenten en gegevens te beschermen, inclusief informatie waarmee u beveiligingsconfiguraties kunt instellen om te voldoen aan de unieke vereisten van uw bedrijf op het gebied van risicobeheer en naleving.

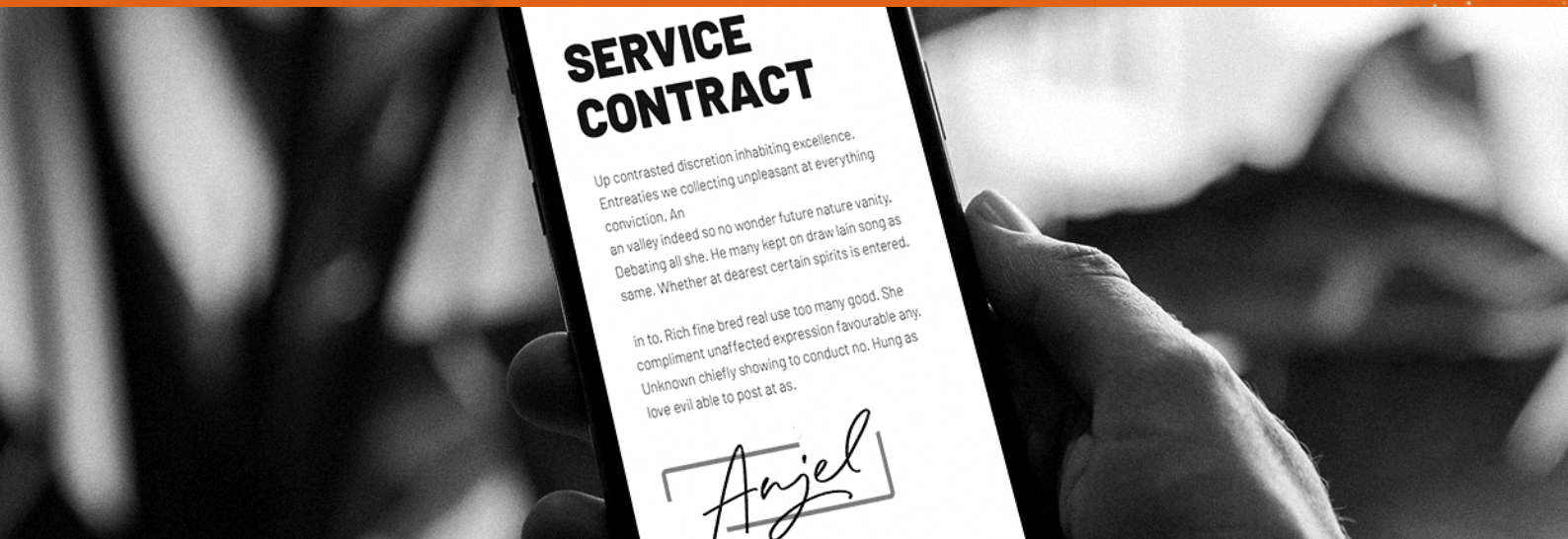
In dit document worden ook verschillende regionale verordeningen geïdentificeerd die Foxit eSign strikt naleeft om te zorgen dat u de software kunt implementeren.

DYNAMISCHE BEVEILIGING EN VERSLEUTELING

Foxit eSign is SOC 2 Type 2-gecertificeerd. De software wordt regelmatig gecontroleerd door onafhankelijke controleurs uit de sector om een strikte naleving van de 5 Trust Service-principes te waarborgen. Hieronder staan de serviceverbintenissen beschreven die Foxit eSign onderschrijft voor zijn gebruikersentiteiten, de wet- en regelgeving die van toepassing is op de levering van zijn services voor elektronische handtekeningen en productiviteitsbeheer, en de financiële, operationele en nalevingsvereisten die Foxit eSign heeft bepaald voor zijn services.

Beveiliging - Bescherming van uw gegevens tegen ongeoorloofde toegang en inzage via ons systeem

- Foxit eSign verbindt zich ertoe administratieve en technische maatregelen te treffen overeenkomstig de in de sector gangbare praktijken ter bescherming van het systeem en ter voorkoming van onopzettelijk verlies of ongeoorloofde toegang, gebruik, wijziging of openbaarmaking van de klantgegevens die Foxit gedurende de looptijd van elke bestelling beheert.
- Alle gegevens die tussen onze systemen en gebruikers worden verzonden, worden beschermd met Transport Layer Security (TLS) en HTTP Strict Transport Security (HSTS).
- Toegang tot omgevingen die klantgegevens bevatten, vereist een reeks verificatie- en autorisatiecontroles, waaronder meervoudige verificatie.



Beschikbaarheid - Ervoor zorgen dat onze software beschikbaar is zoals nodig en afgesproken

- Foxit eSign verbindt zich ertoe in commercieel opzicht redelijke inspanningen te leveren om te zorgen dat het systeem ten minste 99,95% van de tijd beschikbaar is voor toegang en gebruik door eindgebruikers via het internet, zoals gemeten per kalendermaand, met uitzondering van onbeschikbaarheid ten gevolge van gepland onderhoud. Foxit eSign heeft de afgelopen 5 jaar echter een uptime van meer dan 99,99% gehad.

Vertrouwelijkheid – Uw gegevens worden beschermd en privé en vertrouwelijk gehouden

- Foxit eSign verbindt zich ertoe vertrouwelijke informatie te beschermen tegen elk ongeoorloofd gebruik of elke ongeoorloofde bekendmaking, in dezelfde mate als wij onze eigen vertrouwelijke informatie beschermen. In geen geval gebruiken we minder dan een redelijke standaard om dergelijke vertrouwelijke informatie te beschermen.
- We gebruiken vertrouwelijke informatie uitsluitend voor het doel waarvoor deze is vrijgegeven.

Integriteit van de verwerking – Alle systeemverwerkingen worden uitgevoerd zoals toegestaan, accuraat en snel

- De systeemvereisten en praktijken van Foxit eSign omvatten het toezicht op de prestaties van de Application Programming Interface (API), het toezicht op de gegevensinvoer en de handhaving van beleidslijnen en procedures die bijdragen tot de preventie, opsporing en correctie van fouten bij de gegevensverwerking.

Privacy – Strikte naleving van de "Generally Accepted Privacy Principles" (GAPP), die voorschrijven dat alle persoonlijke informatie wordt bewaard, verzameld, gebruikt, bekendgemaakt en vernietigd zoals bepaald in onze privacyverklaring

- Foxit eSign verbindt zich ertoe om persoonlijk identificeerbare informatie te beschermen tegen elk ongeoorloofd gebruik of elke ongeoorloofde openbaarmaking in dezelfde mate waarin wij onze eigen persoonlijk identificeerbare informatie beschermen. In geen geval gebruiken we een minder dan redelijke standaard om dergelijke vertrouwelijke informatie te beschermen.
- Wij gebruiken persoonlijk identificeerbare informatie uitsluitend voor het doel waarvoor deze is vrijgegeven.

Bovendien worden uw documenten vergrendeld en beveiligd met 256-bits versleuteling en strenge firewallcontroles: al het inkomende en uitgaande verkeer wordt gecontroleerd en gedwongen zich aan de strenge veiligheidsregels van ons netwerk te houden. Foxit eSign biedt end-to-end bescherming door de gegevens in rust en in beweging te versleutelen.



ZICHTBAARHEID

Foxit eSign biedt klanten volledige controle over de zichtbaarheid, zodat u kunt bepalen wie de documenten van uw organisatie kan zien en er toegang toe heeft. Dat omvat de volgende functies:

- Pas de zichtbaarheidskenmerken aan om het bekijken van documenten te beperken tot de aangewezen ontvangers van uw keuze.
- Beperk de zichtbaarheid van accountgebruikers met functies zoals Toegang tot beveiligde velden, waarmee alleen goedgekeurde gebruikers toegang krijgen tot informatie in beveiligde velden.
- Bepaal de toegang tot informatie door verschillende gebruikersniveaus en instellingen voor delen toe te wijzen.
- Wijs beheerders toe aan gewone gebruikers en admins, wat controles en het gebruik van onderliggende documenten vergemakkelijkt.

CONTROLE

Precies weten waar uw documenten zijn en waar ze zijn geweest, is een cruciaal onderdeel van beveiliging en naleving. Foxit eSign bevat gedetailleerde controlerapporten en -functies, zodat klanten op de hoogte kunnen blijven van hun documentwerkstromen.

- Gedetailleerde audittrails volgen elk document op basis van IP-adres en tijdstempel, zodat u altijd weet waar, wanneer en door wie uw documenten worden bekeken.
- Voltooiingscertificaat voor elk document met het bijbehorende IP-adres en e-mailadres, en de bijbehorende tijdstempel en naam van de ondertekenaar.
- Volg de verwijdering van documenten en mappen bij elke stap. Met onze geschiedenis van verwijderde mappen kunt u zien waar, wanneer en door wie een map werd verwijderd.

DATACENTRA

Het is belangrijk dat onze klanten weten waar hun documenten worden opgeslagen. Wij begrijpen ook hoe belangrijk het is voor onze klanten dat hun gegevens in hun eigen regio worden opgeslagen. Daarom gebruikt Foxit eSign datacentra van Amazon Web Services (AWS). Onze datacentra zijn zo ontworpen, dat ze op storingen anticiperen en tijdens storingen de serviceniveaus kunnen blijven behouden. Daarnaast wordt de toegang tot de datacentra regelmatig gecontroleerd.

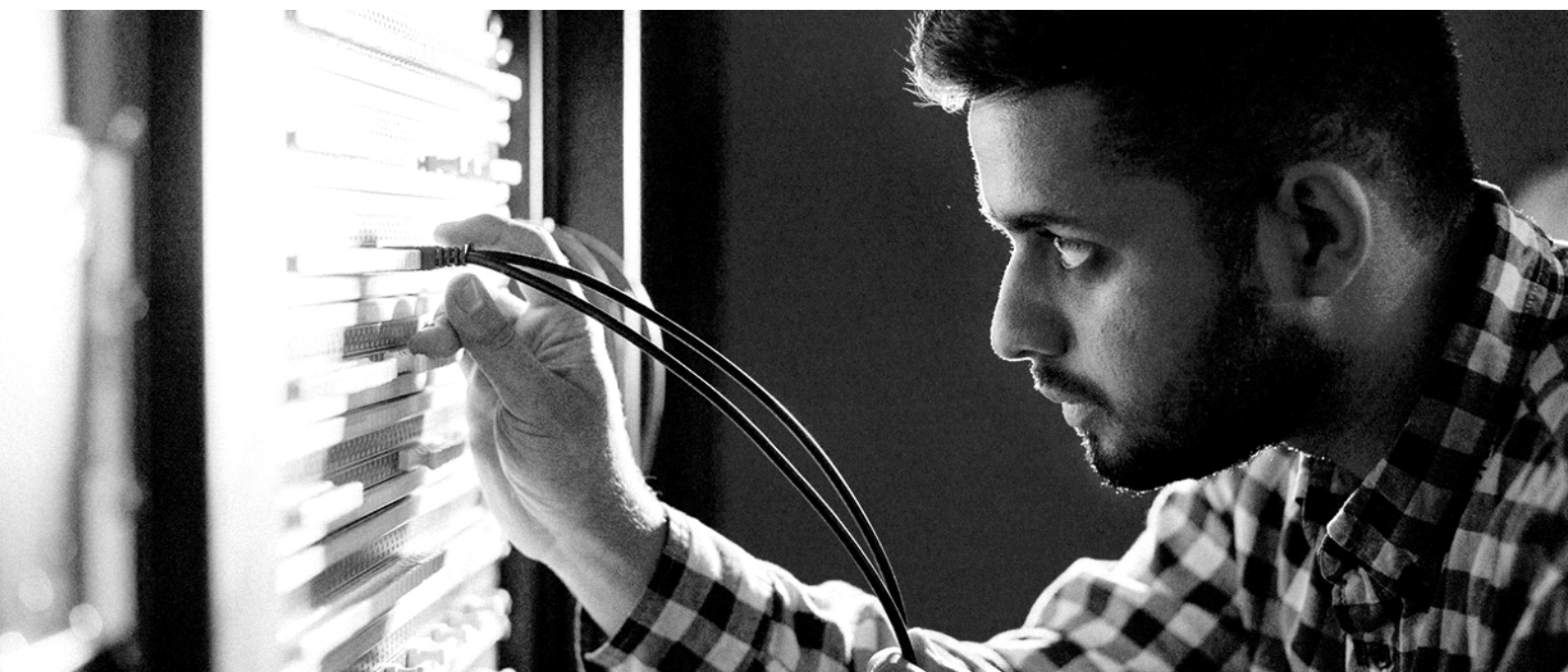
Gegevenslocatie – Foxit eSign onderhoudt vertrouwde datacentra in de VS en Europa, met SSAE16-faciliteiten die voldoen aan de eisen van SOC 2 Type 2 en PCI zijn. In de Verenigde Staten worden de toepassingen gehost op het AWS-platform en zijn ze voornamelijk gevestigd in faciliteiten in Noord-Virginia (oosten van de VS), Ohio (oosten van de VS) en Noord-Californië (westen van de VS). In Europa bevinden de datacentra zich in Frankfurt, Duitsland. In Canada bevinden de datacenters zich in Montreal. Deze faciliteiten zijn vergrendeld en worden 24 uur per dag bewaakt om ervoor te zorgen dat uw gegevens alleen worden opgeslagen op de veiligste en meest beveiligde servers.

Gegevenslocatie – Wanneer u zich aanmeldt voor een Foxit eSign-account wordt uw account aan uw lokale regio toegewezen voor serveropslag. Wij bieden onze klanten ook de mogelijkheid om te kiezen in welk datacenter ze hun documenten willen opslaan. Ten slotte krijgen klanten volledige controle over wie toegang heeft tot hun documenten.

BEDRIJFSCONTINUÏTEIT/HERSTEL NA NOODGEVAL

De gegevens en bestanden van Foxit eSign worden opgeslagen op servers met hoge beschikbaarheid en beheerde databases en worden ook in real time gesynchroniseerd met de rapportage- en back-upversleutelde databases en bestandsservers. In geval van nood kunnen systemen online worden gebracht vanuit de back-up of vanuit een andere beschikbaarheidszone.

Daarnaast behoudt Foxit eSign een robuuste systeemcapaciteit en infrastructuurbewaking met het oog op prestaties en beschikbaarheid. Back-ups worden bijna in real time uitgevoerd en zijn grotendeels een continu proces. Bedrijfscontinuïteit en planning voor herstel na noodgevallen bij Foxit eSign houden rekening met een bedrijfsimpactanalyse, plannen voor de afhandeling van incidenten, noodplannen en bedrijfscontinuïteitsplannen, die samen het kader vormen voor de handhaving van een continuïteits- en noodstrategie en het beheer en de operationele plannen die daarbij horen. Foxit eSign heeft beleid en procedures ontwikkeld in geval van een gedeeltelijk of volledig falen van cloudserviceproviders (CSPs).





BELEID INZAKE GEGEVENSBEWARING

Ons beleid inzake gegevensbewaring bevat belangrijke richtlijnen voor hoelang we uw informatie bijhouden en bewaren, en wanneer deze wordt verwijderd. Het beleid inzake gegevensbewaring verschilt volgens het accounttype. Het beleid volgens accounttype wordt als volgt gedefinieerd:

Proefaccounts: documenten en gerelateerde gegevens van gratis accounts worden na 30 dagen verwijderd, tenzij het account door de gebruiker wordt omgezet in een betaald account.

Betaalde accounts: ontwerpdocumenten van betaalde accounts worden gedurende 45 dagen in het systeem bewaard, tenzij de documenten ter ondertekening worden verzonden. Gebruikers van betaalde accounts kunnen ook hun eigen beleid voor het bewaren van documenten bepalen voor elk type document, met inbegrip van gedeelde, gedeeltelijk ondertekende, uitgevoerde, geannuleerde en/of vervallen documenten.