FOXIT ESIGN. ОБЗОР ФУНКЦИЙ БЕЗОПАСНОСТИ

ТЕХНИЧЕСКОЕ ОПИСАНИЕ

СОДЕРЖАНИЕ

Безопасность является фундаментальным принципом Foxit eSign. Как и во всех наших продуктах, при проектировании и разработке Foxit eSign аспектам безопасности уделялось приоритетное внимание.

В этом документе дан обзор технологий, политик и практик безопасности, которые применяются в Foxit eSign, чтобы защитить документы и данные пользователей, а также содержатся указания по настройке параметров безопасности с учетом уникальных требований компаний к управлению рисками и нормативному соответствию.

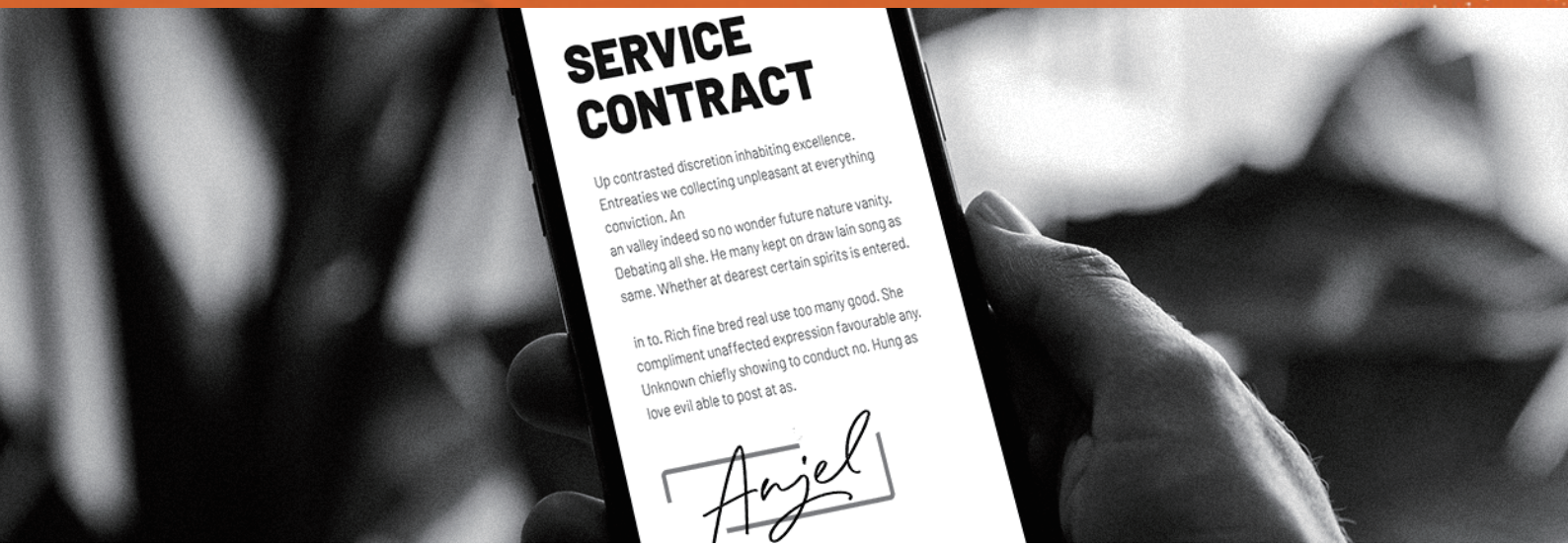
Также в этом документе упомянут ряд региональных нормативов, которым строго следует Foxit eSign, давая пользователям гарантированную возможность развертывания.

ДИНАМИЧЕСКАЯ БЕЗОПАСНОСТЬ И ШИФРОВАНИЕ

Решение Foxit eSign прошло сертификацию SOC 2 Type 2. Для подтверждения строгого соответствия пяти принципам доверительного обслуживания его регулярно проверяют независимые отраслевые аудиторы. Ниже описаны сервисные обязательства Foxit eSign по обслуживанию корпоративных пользователей, соблюдению законов и нормативных актов. Они относятся к функциям электронной подписи и управления производительностью, финансовым и операционным аспектам, а также к требованиям нормативного соответствия, реализованным в Foxit eSign.

Безопасность. Защита данных от неавторизованного доступа и просмотра через нашу систему

- Для защиты системы, предотвращения случайной утраты, несанкционированного доступа, использования, изменения или разглашения клиентских данных, которые находятся под контролем системы в период действия каждого запроса, в Foxit eSign применяются административные и технические меры, отвечающие применимым отраслевым практикам.
- Для защиты всех данных, которыми обмениваются наши системы и пользователи, применяются протоколы безопасности на транспортном уровне (TLS) и строгой безопасности передачи информации по протоколу HTTP (HSTS).
- Для доступа в рабочие среды, в которых содержатся клиентские данные, требуется пройти ряд процедур аутентификации и авторизации, включая многофакторную аутентификацию (MFA).



Доступность. Гарантия доступности нашего программного обеспечения с соблюдением принципа служебной необходимости и согласованных условий

- В Foxit eSign применяются коммерчески обоснованные средства, чтобы обеспечить конечным пользователям доступ к системе и возможность ее использования через Интернет как минимум в течение 99,95% времени на протяжении каждого календарного месяца, исключая периоды недоступности по причине планового технического обслуживания. При этом в последние 5 лет в Foxit eSign поддерживался уровень доступности свыше 99,99%.

Конфиденциальность. Защита, неразглашение и конфиденциальность данных

- В Foxit eSign обеспечивается такая же защита конфиденциальной информации от любого несанкционированного использования и разглашения, которую мы применяем для нашей собственной конфиденциальной информации. В любых обстоятельствах мы будем применять для защиты конфиденциальной информации как минимум разумные стандарты добросовестности.
- Мы используем конфиденциальную информацию исключительно для тех целей, для которых она была предоставлена.

Целостность обработки. Все операции системной обработки выполняются при наличии авторизации, точно и своевременно

- В состав системных требований и практик Foxit eSign входят инструменты контроля эффективности программного интерфейса (API), мониторинг вводных данных, а также политики и процедуры, которые помогают выявлять, предотвращать и исправлять ошибки при обработке данных.

Неразглашение. Строгое соблюдение общепринятых принципов неразглашения, которые требуют, чтобы сбор, удержание, использование, раскрытие и уничтожение всей персональной информации осуществлялись в соответствии с нашим уведомлением о неразглашении.

- Информация, позволяющая идентифицировать личность, защищается в Foxit eSign от любого несанкционированного использования и разглашения на том же уровне, на котором мы защищаем свою собственную информацию данной категории. В любых обстоятельствах мы будем применять для защиты информации, позволяющей идентифицировать личность, как минимум разумные стандарты добросовестности.
- Мы используем информацию, позволяющую идентифицировать личность, исключительно для тех целей, для которых она была предоставлена.

В дополнение к этому, документы блокируются и защищаются с применением 256-битного шифрования отраслевого уровня, и действует строгий контроль на межсетевых экранах. Весь входящий и исходящий трафик должен проходить мониторинг и подчиняться жестким правилам безопасности, установленным в нашей сети. Для целей сквозной защиты данные в Foxit eSign шифруются как в неподвижном состоянии, так и в движении.

ВИДИМОСТЬ

В Foxit eSign пользователям предоставлены все инструменты контроля, позволяющие выбрать, кто будет иметь право просмотра и доступа к документам организации. В частности, это:

- настраиваемые функции видимости, которые ограничивают возможность просмотра только заданным кругом получателей,
- ограничение видимости с привязкой к учетным записям пользователей, например с помощью функций доступа к защищенным полям, которые открывают доступ к данным в таких полях только при наличии разрешения,
- контроль над доступом к информации с назначением разных уровней и настроек совместного доступа,
- назначение менеджеров регулярным пользователям и администраторам для простоты и удобства мониторинга и субординации документооборота.

АУДИТ

Точная информация о том, где находятся и находились документы, является важнейшим элементом безопасности и нормативного соответствия. В Foxit eSign доступны подробные аудиторские отчеты и функции, благодаря которым клиенты получают актуальную информацию о документообороте.

- Подробный аудиторский след содержит идентификацию каждого документа с IP-адресами и метками времени. Пользователям доступен полный объем информации о том, когда, где и кто просматривал их документы.
- Каждый документ сопровождается сертификатом оформления с указанием IP-адреса, электронной почты, метки времени и имени подписавшего лица.
- На каждом этапе отслеживается удаление документов и папок. В истории удаления указано, где, когда и кем была удалена любая конкретная папка.

ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ

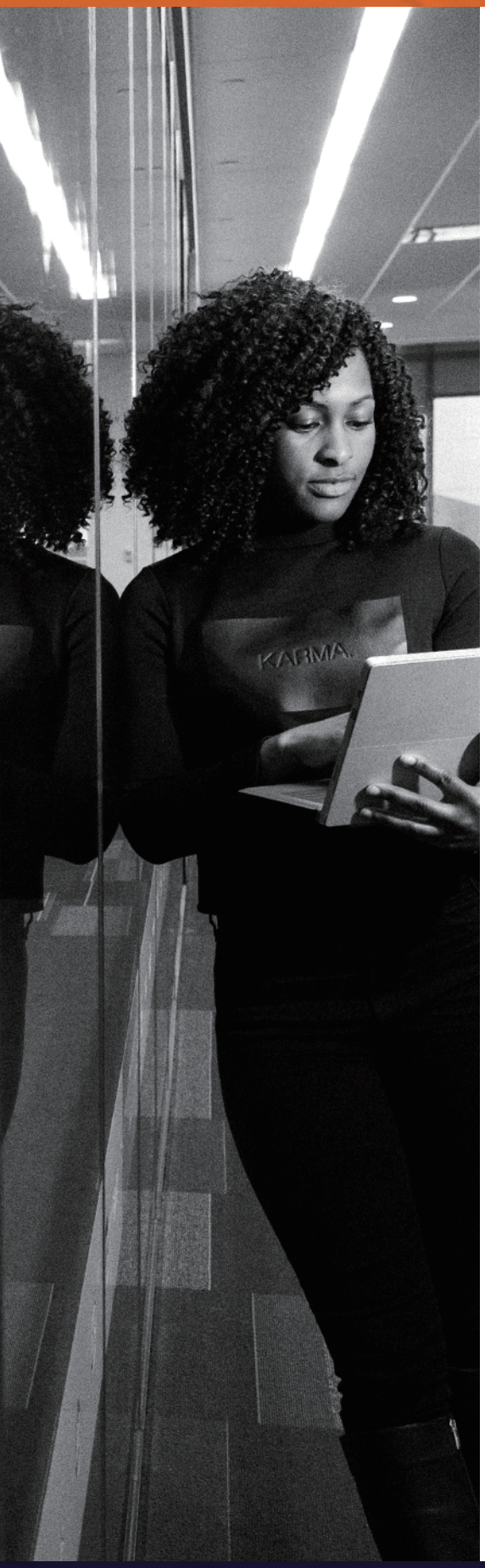
Важно, чтобы наши клиенты имели представление о том, где хранятся их документы. Также мы понимаем, насколько значимую роль для них играет локальное размещение данных. По этим причинам в Foxit eSign используются центры обработки данных Amazon Web Services (AWS). При проектировании наших центров обработки данных учитываются и закладываются параметры отказоустойчивости, регулярно контролируются доступность и уровни обслуживания.

Местонахождение данных. В Foxit eSign используются доверенные центры обработки данных на территории Европы и США, отвечающие требованиям SSAE16, SOC 2 Type 2 и PCI. В США приложения размещаются на платформе AWS и в основном работают на объектах, находящихся в Северной Виргинии (восток страны), Огайо (восток страны) и Северной Калифорнии (запад страны). В Европе центры обработки данных располагаются в немецком Франкфурте. Это закрытые объекты, находящиеся под круглосуточным наблюдением. В Канаде центры обработки данных располагаются в Монреале. Данные пользователей гарантированно хранятся только на самых надежных и безопасных серверах.

Резидентство данных. Для целей серверного хранения при регистрации в Foxit eSign учетная запись пользователя привязывается к его локальному региону. Также мы предоставляем нашим клиентам возможность выбрать предпочтительный центр обработки данных для хранения документов. И, наконец, клиенты получают полный контроль над кругом лиц, которым предоставляется доступ к их документам.

НЕПРЕРЫВНОСТЬ ДЕЯТЕЛЬНОСТИ И ПОСЛЕАВАРИЙНОЕ ВОССТАНОВЛЕНИЕ

Данные и файлы в Foxit eSign хранятся на высокодоступных серверах и в управляемых базах данных, а также синхронизируются в реальном времени с зашифрованными базами данных, файловыми серверами отчетности и резервного копирования. В аварийных ситуациях системы могут быть восстановлены онлайн из резервной копии или другой зоны доступности.



Также для обеспечения доступности и результативности в Foxit eSign заложены мощные системные ресурсы и мониторинг инфраструктуры. Процесс резервного копирования выполняется в режиме, приближенном к реальному времени, в основном непрерывно. При планировании непрерывности деятельности и послеаварийного восстановления в Foxit eSign учитываются результаты анализа воздействия на бизнес, планы по отработке инцидентов, действиям в экстренных ситуациях и обеспечению непрерывности. В совокупности они формируют рамочные основы для стратегии непрерывности и экстренных действий, планов управления и операционной деятельности. В Foxit eSign разработаны политики и процедуры на случай частичного или полного сбоя в работе провайдеров облачных служб.

ПОЛИТИКА УДЕРЖАНИЯ ДАННЫХ

Наша политика удержания данных устанавливает важные правила в отношении сроков отслеживания, хранения и утилизации пользовательских данных. Действуют разные политики удержания, выбираемые в зависимости от типа учетной записи. Предусмотрены следующие варианты.

Учетные записи для пробного использования: документы и сопутствующие данные, привязанные к бесплатным учетным записям, удаляются через 30 дней, если пользователь не перешел на платную учетную запись.

Платные учетные записи: если документы не отправлены на подпись, черновики, привязанные к платным учетным записям, хранятся в системе в течение 45 дней. Также пользователи с платными учетными записями могут настраивать собственные политики удержания для документов разных типов, например открытых для совместного доступа, частично подписанных, оформленных, отмененных и/или с истекшим сроком действия.

Foxit
Lennéstr. 1
10785 Berlin, Germany

Отдел сбыта: +49 30 234849944
или +49 30 234849945
Служба поддержки: +49 30 21783691

Центр поддержки
www.foxit.com