Dropbox DocSend security, legality, and privacy

A Dropbox whitepaper

Dropbox DocSend

Table of contents

Introduction

Dropbox DocSend is the secure document sharing platform everyone can use. We make managing, sharing, and tracking your important files as easy as sharing a link. From email authentication to an embedded NDA, DocSend's advanced document security features have you and your sensitive information covered. In addition to DocSend's document-level analytics, which gives you insight into who's viewed your document and where specifically they've spent time, DocSend's advanced security features include allowlisting (limiting access to your content by domain or email address), watermarking, document viewer email verification, and one-click NDAs that make signing an NDA mandatory before viewing a confidential document. Control every aspect of your shared files—even after you hit send—with DocSend.

DocSend services are designed with a secure, distributed infrastructure with multiple layers of protection. We work to ensure your data is protected, and empower our customers with tools that provide control and visibility.

You can learn more about DocSend product features below, in **Product Information.**

Dedicated and experienced security team

Our security program is designed to assess risks and build a culture of security at DocSend. Every single employee at Dropbox is dedicated to security and protecting our customer data in all that we do. DocSend Services are in alignment with the information security program in place under the Head of Security at Dropbox. As part of our formal risk management program, security risks are reviewed periodically, resulting in security-related initiatives at the product, infrastructure, and company level.

The Privacy Team is responsible for operating the Privacy Program. They implement our key privacy initiatives and champion privacy-by-design in our data lifecycle.

To ensure all Dropbox employees are able to foster customer data protection, we work to ensure security and privacy are embedded in our company culture from day one. Employees undergo comprehensive background checks, sign and follow a code of conduct and acceptable use policies, and undergo annual security awareness and privacy training. Continuous information security awareness is maintained via monthly information security newsletters and security relevant notifications.

Reliability

When you're doing business, you need us to be there for you. That's why we strive to hit the highest uptime possible.

Business continuity and disaster recovery

The company is aware that disasters can strike at any time and in any region or location. The infrastructure is designed for resilience, and contingency plans are in place in case of service-impacting events. We use Amazon Web Services (AWS), which is dispersed across multiple data centers for data and processing redundancy. The company has a comprehensive business continuity and disaster recovery plan to ensure system availability. The Business Continuity and Disaster Recovery Plan is reviewed and tested on an annual basis. Critical data related to the system is backed up on a continuous basis. Engineering is notified in the event of backup failure, and issues are resolved as appropriate.

Authentication

It's extremely important that we verify a user is who they say they are before being allowed to access protected documents. To that end, we have several capabilities that ensure strong authentication of individuals.

All passwords are securely hashed and salted

- ***Single Sign-On***

  DocSend can be configured to allow team members access by signing into a central identity

provider. Our SSO implementation, which uses the industry-standard Security Assertion Markup Language 2.0 (SAML 2.0), makes provisioning easier and more secure by placing a trusted identity provider in charge of authentication and giving team members access to Dropbox without an additional password to manage.

- ***DocSend product specific authentication features***

  Password-protected file sharing: users can set a passcode, verify via email, and restrict access to ensure only the right people can view their files. Users can also set expiration dates and turn on or off the ability to download the files.

  Gate access with agreements: users can gate access to content with an agreement, such as an NDA.

Permissions

It's imperative that you can control who can do what within the system.

DocSend product

Different roles carry different access rights. For example, Administrators control team-wide settings, billing information, and roles.

- ***Role-based security:*** enables different levels of permissions for different members of a team, ranging from administrative rights to members.
- ***Sub-teams:*** DocSend sub-teams allow users to grant access to specific content that is relevant to each team within an organization. Sub-teams keep sensitive content secure and ensure that only authorized users have access to it.

Encryption

DocSend protects data in transit, between our apps and our servers, and at rest. Documents are stored behind a firewall and authenticated against the sender's session every time a request for that document is made. We enforce the use of industry best practice for the transmission of data to our platform, Transport Layer Security (TLS), and data is stored in SOC 1 Type II, SOC 2 Type II, and ISO 27001 certified data centers. Documents are stored and encrypted at rest using AES 256-bit encryption. Documents are transferred using a presigned, expiring URL to upload content.

Privacy

At Dropbox DocSend we believe that you own your data, and we're committed to keeping it private. Our Privacy Policy clearly describes how we handle and protect your information. On an annual basis, our independent third-party auditors test our privacy-related controls and provide their reports and opinions, which we can provide to you upon request.

For any privacy-related questions, please contact privacy@dropbox.com.

Application security

DocSend has a formal application security program in place with application security staff. We regularly test our infrastructure and apps to identify and patch vulnerabilities. We also work with third-party specialists, industry security teams, and the security research community to keep our users and their files safe. To further enhance our application security, we run a bug bounty program and engage multiple times a year with third-party penetration testing teams to ensure our products are secure. Potential security bugs and vulnerabilities can be reported to our Security and Abuse Bug Bounty program, which is offered through Bugcrowd: bugcrowd.com/dropbox.

Security monitoring

DocSend uses a cloud native security platform to monitor the security of its production environment and actively monitors for suspicious user activity.

Infrastructure / physical security

DocSend uses Heroku as its Platform as a Service (PaaS) provider and Amazon Web Services (AWS) as its Infrastructure as a Service (IaaS) provider with Amazon data centers hosting our data within the U.S.

Amazon Web Service (AWS) operates state-of-the-art SOC 1 Type II, SOC 2, and ISO 27001 certified facilities. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards.

We utilize AWS features like Security Groups, key management, disk level encryption, etc., to ensure the confidentiality of our customer data in the cloud.

Our subservice providers

At least annually, Dropbox DocSend performs a review of our subservice providers. In the event these reviews have material findings which we determine present risks to DocSend or our customers, we will work with the service provider to understand any potential impact to customer data and track their remediation efforts until the issue is resolved.

Our Privacy Policy explains the limited circumstances under which your data may be shared with third parties. For purposes of the CCPA, DocSend does not “sell” Personal Data, nor do we have actual knowledge of any “sale” of Personal Data of minors under 16 years of age.

Compliance

At Dropbox DocSend we believe that compliance is an effective way to validate a service’s trustworthiness. We comply with standards and regulations like SOC 2. On an annual basis our independent third-party auditors test our controls and provide their reports and opinions, which we can provide to you upon request.

DocSend's systems are annually audited for compliance with the requirements of SOC 2 stipulated by the American Institute of Certified Public Accountants (AICPA).

Amazon's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

In addition, DocSend has completed the rigorous security review process put in place by Salesforce as part of being listed on the Salesforce AppExchange.

Please contact us (via email: support@docsend.com) for access to our audits and assessments.

Security incidents & reporting

If you need to submit a potential security incident to DocSend, please contact the Dropbox DocSend Security Team: security@docsend.com. The team will evaluate the report and may arrange to discuss specifics.

Links to important resources

Terms of Service
Privacy Policy
Copyright and IP Policy
Cookie Policy

Product information

Dropbox DocSend provides a wide range of features, which vary by plan. For more information, see Dropbox DocSend Pricing. Depending on plan type, features that our users have access to include:

Secure file sharing
Control every aspect of shared files, enable secure file sharing with DocSend links and passcodes, and set expiration dates for downloads.

Dynamic watermarking
Helps prevent unwanted sharing, displays viewer info, and more.

Virtual data rooms
Virtual data rooms (VDRs) enable sharing multiple documents with a single link and provides viewers with content and ability to upload files with or without a DocSend account. They can support specified email addresses and domains, as well as passcodes and NDA signatures.

eSignature
Convert files to signable documents, or create them directly from DocSend. Complies with E-Sign and UETA regulations and supports multiple users and the analytics associated with their document interactions.

NDAs
Set up NDAs or other agreements for sensitive content, requiring viewers to provide a signature before accessing a document.

User roles
Use multiple levels of user access, including role-based security permissions. Users range from members who upload and update content to the admins who manage them and their accounts. Some plans also include an owner, who can access the Billing page and transfer account ownership.

User management
Keep documents secure and billing current. DocSend Owners and Admins can add, deactivate, suspend, and reactivate users.

Transfer user data
DocSend Owners and Admins can use Transfer User Data to move all of a suspended or deactivated user's data to another active user, ensuring that the inactive user's links and documents remain accessible.

Single Sign-On (SSO)
Teams can log in securely through Okta or OneLogin via SAML 2.0, with which DocSend also supports SCIM for user provisioning.

Sub-teams
Use Sub-teams to organize and grant access to specific content that's relevant to each team within an organization. This helps keep content secure and ensure that only authorized users can access it. Folder access can be managed by sub-teams as well.