Dropbox Sign Services Security, Legality, and Privacy

Dropbox Sign

Table of Contents

Table of Contents

Introduction

The documents, contracts, and agreements you sign as a business are some of the most important documents you have. Many of these types of transactions involve a legally-binding signature and are critical in a company's operations. Examples include new employee hiring documents, sales contracts, building leases, partner relationships, vendor agreements, and so much more. These documents often contain sensitive information, so security is a primary concern. With Dropbox Sign Services, which includes Dropbox Sign, Dropbox Forms, and Dropbox Fax, protection of your documents and related transactions are the highest priority. We are committed to ensuring the privacy, security, and protection of every document that is signed using Dropbox Sign Services.

Security covers a very broad range of topics, and this white paper provides a fairly thorough overview of all of them. For customers purchasing a certain minimum contract value, Dropbox can work with you on customized security reviews, questionnaires, and assessments.

Dedicated and Experienced Security Team

Every single employee at Dropbox is dedicated to security and protecting our customer data in all that we do. Dropbox Sign Services is in alignment with the information security program in place under the Head of Security at Dropbox.

At Dropbox, employees undergo comprehensive background checks, sign and follow a code of conduct and acceptable use policy, as well as undergo annual security awareness and privacy training.

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. You can always see our current availability at our **status site**.

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 daily 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 either issue a document for signature or execute a signature. To that end, we have several capabilities that ensure strong authentication of individuals.

2-Factor Authentication.

Users are able to set up 2-Factor Authentication, which requires the entry of a unique code generated via Google Authenticator or sent to the individual via SMS. This code must be used in addition to their username and password. Team admins can mandate which method is used for 2-Factor Authentication.

- **Single Sign-On** is available using a Dropbox or Google account.
- **API key-based authentication for the API.**
- **All passwords are securely hashed and salted.**

Sessions expire after a certain time.

1 hour by default, which can be extended to 30 days if the user selects **Remember Me** during login.

Dropbox Sign product specific authentication features:

- **Access Code protected signature requests.** For the Dropbox Sign product, users can enable a Signer Access Code (a 4 through 12 character alpha numeric string) that signers must enter in order to view a document.

- **OAuth**. The Dropbox Sign API supports OAuth as a means of authenticating API calls on behalf of a user.

- **SAML**. Dropbox Sign supports SAML 2.0 for enterprise single sign-on

Permissions

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

Dropbox Sign Product

Different roles carry different access rights, both in the Dropbox Sign API and in the end user product. 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 who have only permissions to view templates and issue signature requests.

- **Signer-specific access codes**. As an extra layer of security, each signer can be assigned a Signer Access Code for additional assurance of who is signing.

Dropbox Forms Product

- **Role-based security.** Enables different levels of permissions for different members of a team, ranging from administrative rights to members with limited access to functionality.

Encryption

Documents are stored in a securely controlled infrastructure and authenticated against the sender's session every time a request for that document is made. We enforce the use of industry best practices for the transmission of data to our platform (Transport Layer Security or TLS) and data is stored in SOC 1 Type II, SOC 2 Type I, and ISO 27001 certified data centers. Your documents are stored and encrypted at rest using AES 256-bit encryption.

In addition, each document is encrypted with a unique key. As an additional safeguard, each key is encrypted with a regularly-rotated master key. This means that even if someone were able to bypass physical security and remove a hard drive, they wouldn't be able to decrypt your data.

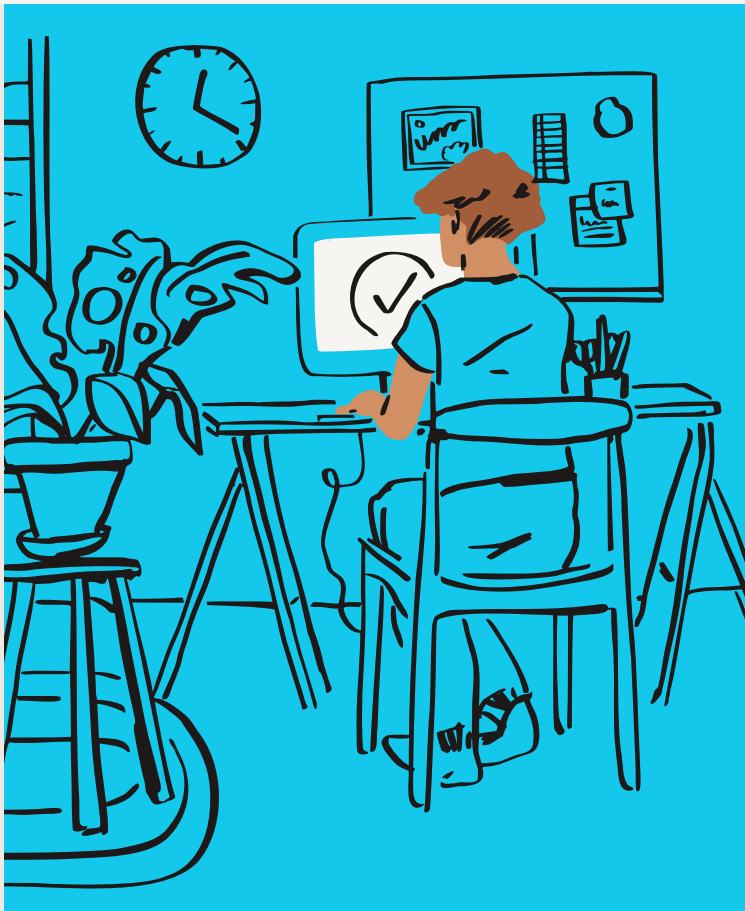
In summary:

- All documents are encrypted at rest using AES-256.
- Each document is encrypted using a unique key, which is itself encrypted with a master key.
- The master key is rotated regularly.
- Backups of documents are encrypted.
- Documents in transit are encrypted using TLS 1.2 or later.
- The web application has HSTS configured to ensure a secure connection.

Privacy

At Dropbox 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. You can find more information about how Dropbox is committed to protecting your personal data **here**.

To report a privacy-related issue, please contact: privacy@dropbox.com.



Audit Trail

Dropbox Sign Product

Each signature on a contract is imposed and affixed to the document. When you request a signature, Dropbox Sign affixes an audit trail page to the document itself. The audit trail contains a globally unique identifier (GUID) that can be used to look up a record in our database, showing who signed a document and when. Read our **statement of legality** for more details.

The non-editable audit trail ensures that every action on your documents is thoroughly tracked and time-stamped, to provide defensible proof of access, review, and signature.

There are a number of different audit-tracked events in Dropbox Sign, including:

- Document Sent
- Document Viewed
- Document Signed
- Decline to Sign
- Signer Name/Email Address Updated
- Attachment Uploaded
- In-person Signing Activated
- Signer Access Code Authenticated
- Electronic Record and Signature Disclosure Accepted
- Signature Request Delegated
- Signature Request Completed
- Completed Request Continued

A current list of all audit-tracked events can be found on our **security page**.

Authenticity

Each signature on a contract is imposed and affixed to the document. When you request a signature, Dropbox Sign affixes an audit trail page to the document itself. The audit trail contains a globally unique identifier (GUID) that can be used to look up a record in our database, showing who signed a document and when. Read our statement of legality for more details.

Application Security

Dropbox Sign Services application security is fully integrated with the Dropbox Application Security program. We perform design and architecture reviews of new features through our intake process. All Dropbox Sign Services code is scanned for security related issues using static code analysis tools like Semgrep & CodeScan. Dropbox Sign Services is also covered under our Security and Abuse Bug Bounty program, which is offered through Bugcrowd: **bugcrowd.com/dropbox**.

Security Monitoring

Dropbox Sign Services uses cloud-native security platforms, with direct alert escalation for Dropbox Security. Dropbox actively monitors for suspicious user activity and tracks access to critical components.

Infrastructure

Dropbox Sign Services uses Amazon Web Services (AWS) as its Infrastructure as a Service (IaaS) provider with Amazon Data Centers hosting our data within United States. We also make use of AWS regions in EU, UK, JP, AU, and CA.

Dropbox Sign Services utilizes Amazon security features like Virtual Private Cloud (VPC), Security Groups, disk level encryption, and others to ensure the confidentiality of our customer data in the cloud.

Physical Security

Dropbox Sign Services is hosted in Amazon Web Services, which operates state-of-the-art SOC 1 Type II, SOC 2 and ISO 27001 certified facilities.

Personnel Security

All Dropbox employees undergo comprehensive background checks before joining. All employees and contractors have to sign and follow a code of conduct and an acceptable use policy. All employees must complete information security awareness and privacy training upon joining and on an annual basis. Continuous information security awareness is maintained via information security newsletters and security relevant notifications.

Compliance

Dropbox Sign adheres to the following frameworks, standards, and regulations:

SOC 2 Type II

Service Organization Controls (SOC) Reports are frameworks established by the American Institute of Certified Public Accountants (AICPA) for reporting on internal controls implemented within an organization. Dropbox Sign has validated its systems, applications, people, and processes through an audit by an independent third-party, Schellman Compliance LLC.

The SOC 2 report provides customers with a detailed level of controls-based assurance, covering the Trust Service Criteria for Security, Availability, and Confidentiality (TSP Section 100). The SOC 2 report includes a detailed description of Dropbox Sign's processes and the more than 100 controls in place to protect your customer data. In addition to our independent third-party auditor's opinion on the effective design and operation of our controls, the report includes the auditor's test procedures and results for each control. The SOC 2 examination is available upon request through our sales team by emailing compliance-reports@hellosign.com.

ISO 27001 (Information Security Management)

ISO 27001 is recognized as the premier information security management system (ISMS) standard around the world. The standards also leverage the security best practices detailed in ISO 27002. To be worthy of your trust, we're continually and comprehensively managing and improving our physical, technical, and legal controls at Dropbox Sign. Our auditor, Schellman Compliance LLC, maintains its ISO 27001 accreditation from the **ANSI-ASQ National Accreditation Board (ANAB)**. View the Dropbox Sign, Dropbox Fax, and Dropbox Forms **ISO 27001 Certificate**.

ISO 27018 (Cloud Privacy and Data Protection)

ISO 27018 is an international standard for privacy and data protection that applies to cloud service providers, like Dropbox Sign, who process personal information on behalf of their customers and provides a basis for which customers can address common regulatory and contractual requirements or questions. Our adherence to ISO 27018 is validated as part of our ISO 27001 certification. View the Dropbox Sign, Dropbox Fax, and Dropbox Forms **ISO 27018 Certificate**.

Our Dropbox Sign and Dropbox Forms products support HIPAA compliance

Dropbox Sign supports Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) compliance.

These laws aim to encourage the proliferation of technology in the health care industry, while building protections for the security and privacy of health information. Organizations like hospitals, doctors' offices, and dental practices, as well as individuals who interact with protected health information (PHI) may be subject to HIPAA/HITECH. This may also extend to companies that work with these businesses and come into contact with PHI on their behalf.

Dropbox Sign makes available a report related to HIPAA Security Rule and HITECH Breach Notification Requirements. Customers interested in requesting these documents can reach out to our sales team by emailing compliance-reports@hellosign.com.

The U.S. ESIGN Act of 2000

The Electronic Signatures in Global and National Commerce Act is a federal law that provides a general rule of validity for electronic records and signatures for transactions. Among other things, The US ESIGN Act requires demonstration of an intent to sign, certain consumer disclosures, and record retention.

The Uniform Electronic Transactions Act (UETA) of 1999

Passed in 1999 by the National Conference of Commissioners on Uniform State Laws, the **Uniform Electronic Transaction Act** allows the use of electronic communication transactions by giving electronic signatures the same legal weight as handwritten pen to paper signatures. The UETA has been adopted by every state except New York.

IDAS Regulation (eIDAS regulation for the EU of 2016 (EU Regulation 910/2014), which replaced the former European EC/1999/93 Directive)

The eIDAS regulation defines three types of electronic signature (SES, AES, QES) and is a regulation on electronic identification and trust services for electronic transactions in the European Single Market. It establishes a legal framework for people, companies (in particular small to mid-size enterprises) and public administrations to safely access services and execute transactions digitally across all the EU member states. Dropbox Sign supports SES and QES electronic signatures. Find more information about eIDAS on our **compliance page**.

Privacy Shield

Dropbox complies with the EU-U.S. and Swiss-U.S. Privacy Shield frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data transferred from the European Union, the European Economic Area, and Switzerland to the United States. View the Dropbox **Privacy Shield certification** and learn more at the **Privacy Shield website**.

EU General Data Protection Regulation (GDPR)

The General Data Protection Regulation 2016/679, or GDPR, is a European Union regulation that marked a significant change to the existing framework for processing personal data of EU data subjects. The GDPR introduced a series of new or enhanced requirements that applies to companies like Dropbox, which handle personal data. Dropbox Sign adheres to GDPR so that customers can use Dropbox Sign to facilitate their GDPR compliance. Get the full details on **GDPR and Dropbox Sign compliance** in our trust center.

Please contact us (via email: compliance-reports@hellosign.com) for access to our audits and assessments.

Links to Important Resources

Dropbox Sign Privacy Policy

Dropbox Sign Trust Center

Dropbox Sign Security

Dropbox Sign Compliance