HELLOSIGN
a Dropbox Company

HelloSign Security, Legality and Privacy

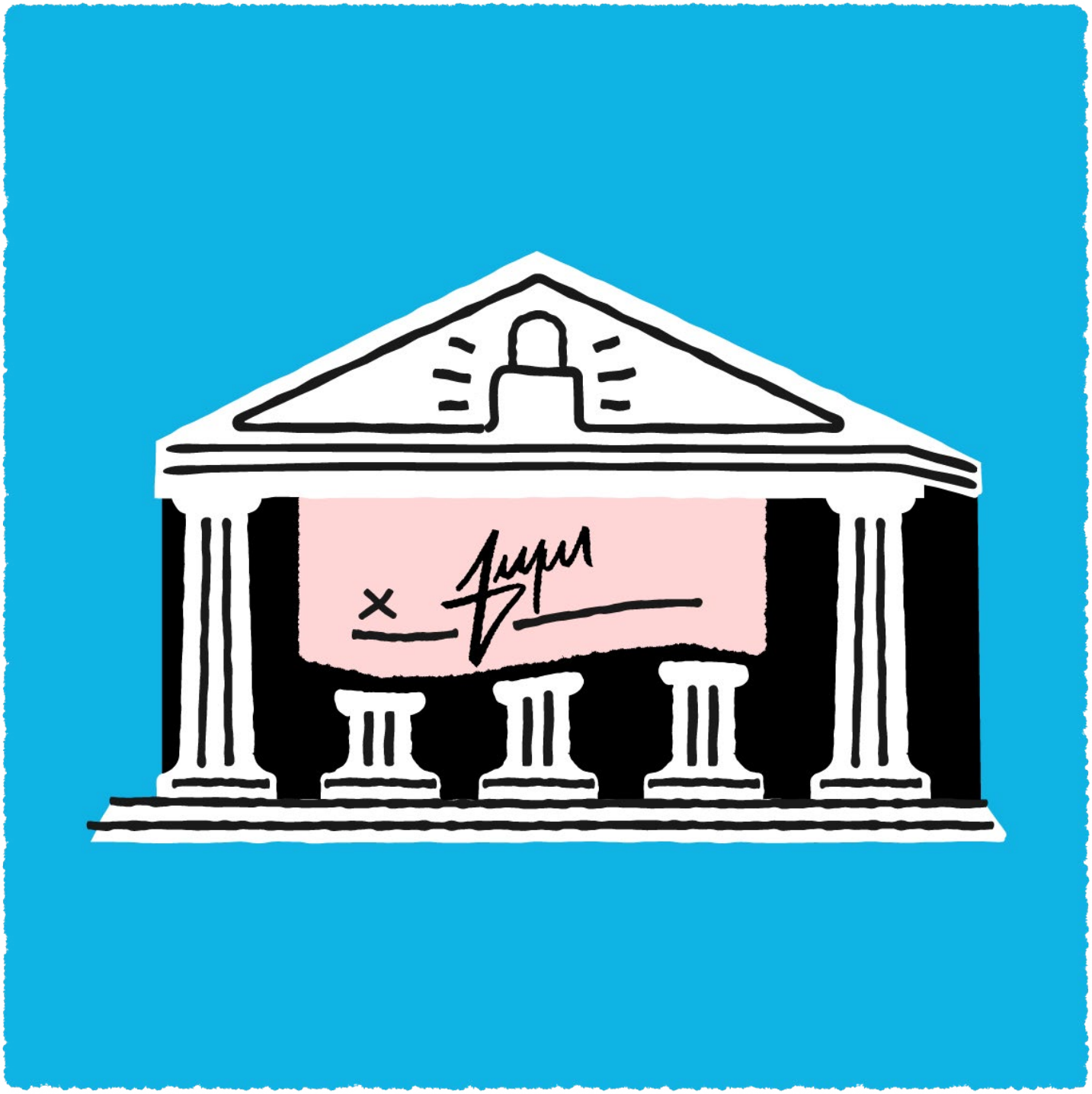

Table of Contents

Introduction

The documents, contracts and agreements you sign as a business are some of the most important documents you have. In fact, transactions that involve a legally binding signature often represent some of the most important in a company's operations - new employee hiring documents, sales contracts, building leases, partner relationships, vendor agreements, and so much more. More often than not these documents contain sensitive information so security is a primary concern. At HelloSign, protection of your documents and related transactions are of the highest priority. We are 100% committed to ensuring the privacy, security, and protection of every document that is signed with our service.

Security covers a very broad range of topics, and this datasheet is meant to give you a fairly thorough overview of all of them. For prospects and customers purchasing a certain minimum contract value, HelloSign can work with you on customized security reviews, questionnaires, and assessments.

– Neal O'Mara, Co-Founder & Chief Technology Officer at HelloSign

HelloSign Security, Legality and Privacy

DEDICATED AND EXPERIENCED SECURITY TEAM

Every employee at HelloSign, from office operations to our CEO, is dedicated to security and protecting our customer data in all that we do.

HelloSign has a formal information security program in place under the Head of Security who leads the Information and Risk Management Committee. This committee periodically meets to review security-related initiatives at the product, the infrastructure, and the company level.

At HelloSign employees undergo comprehensive background checks, sign and follow a code of conduct and acceptable user policy, as well as undergo annual security awareness 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. AWS 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. The DevOps Team is notified in the event of backup failure and issues are resolved as appropriate.

AUTHENTICATION

It's extremely important to verify users and email addresses before completing a signature request. We provide capabilities for our customers to authenticate users to

ensure genuine signatures on signed documents.

- **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 that individual via SMS, along with their username and password.
- **API key-based authentication for the API**
- **All passwords are securely hashed and salted**
- **Sessions expire after a certain time**
- **HelloSign product specific authentication features:**

    1. **Password-protected signature requests** - For the HelloSign product users can enable a 4-12 digit pin code that signers need to enter in order to view a document.
    2. **OAuth** - The HelloSign API supports OAuth as a means of authenticating API calls on behalf of a user.

PERMISSIONS

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

HelloSign Product
Different roles carry different access rights, both in the HelloSign API and in the end user product. For example, Administrators control team-wide settings, billing information, and the roles of others.

- **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 -** Can be assigned to each individual being asked to sign as an extra layer of security

HelloWorks Product
The HelloWorks is designed to be a workflow product as such the HelloWorks product supports a single role. All users with access to an account will have the same privilege within a team. Access to teams require an invite from the team owner.

ENCRYPTION

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 a 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.

- **All documents are encrypted at rest using AES 256-bit encryption**
- **For any document in transit to be signed, communications are encrypted using industry best practice (Transport Layer Security TLS)**
- **All backups are encrypted**
- **HSTS is enabled (HTTP Strict Transport Security)**
- **We use 2 levels of document encryption - Each document is encrypted using a unique key (a document encryption key or DEK), and that DEK is then encrypted using a master key that is regularly rotated**

Privacy

At HelloSign 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 then provide to you.

Here are a few of the ways we protect your data:

Data Deletion/Destruction

Upon request, HelloSign will work to expunge all customer data and solely owned artifacts from our systems. Artifacts under legal hold or owned by multiple parties will be deleted upon completion of the legal hold process or upon deletion by all other parties at their discretion.

Payment Info

We process all payments through our payment provider, Stripe, and do NOT store cardholder data on our servers. HelloSign is PCI compliant merchant for payment processing.

Our privacy policy can be found here.

SECURE AUDIT TRAILS

HelloSign

Each signature on a contract is imposed and affixed to the document. When you request a signature, HelloSign affixes an audit trail page to the document itself. The audit trail contains a globally unique identifier, or GUID, that can be used to look up a record in our database that shows who signed a document and when. These records include a hash of the PDF document which we can compare to the hash of a questionable PDF document to determine whether or not it has been modified or tampered with. Our statement of legality can be found here.

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.

Here are a list of all audit-tracked events in HelloSign:

- Document Uploaded
- Document Viewed
- Document Removed
- Document Sent
- Document Signed
- Signer Email Address Updated
- Signer Access Code Authenticated
- Signature Request Canceled
- Attachment Uploaded
- Signature Request Declined
- E-Sign Disclosure Opt-In

APPLICATION SECURITY

HelloSign has a formal application security program in place with dedicated application security staff. All code is scanned for security related issues using static code analysis tools. To further enhance our plication security, HelloSign runs a bug bounty program and we engage multiple times a year with third-party penetration testing teams to ensure our products are secure.

SECURITY MONITORING

HelloSign uses a cloud native security platform to monitor the security of its production environment. HelloSign actively monitors for suspicious user activity, and tracks access to key secret and configuration files.

INFRASTRUCTURE

HelloSign uses Amazon Web Services (AWS) as its Infrastructure as a Service (IaaS) provider with Amazon data centers hosting our data within United States.

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

PHYSICAL SECURITY

HelloSign is hosted in a state-of-the-art SOC 1 Type II, SOC 2 and ISO 27001 certified facility. Physical access is strictly controlled by professional security staff utilizing video surveillance, state-of-the-art intrusion detection systems, and other electronic means. Authorized staff must pass 2-Factor authentication no fewer than three times to access data center floors.

PERSONNEL SECURITY

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

INTERNAL POLICIES, PROCEDURES, AND REPORTS

HelloSign adopts and adheres to several internal procedures that make sure the way we build, test, and release our software is with our customers' security and scalability needs in mind. Here is a list of our internal policies, procedures and reports which may be shared under one-way NDA if needed during an evaluation process:

- Information Security Policy
- Acceptable Use Policy
- Code of Conduct
- Incident Response Plan
- Business Continuity and Disaster Recovery Plan
- Breach Notification Policy
- Technology, Cyber, Data Risk, and Media Insurance Declarations
- SOC 2 Type II Report
- Penetration test executive summary reports
- PCI DSS Self Attestation
- ISO 27001 Certificate

COMPLIANCE

In order to meet the most stringent security and compliance needs of our customers around the world, it's imperative that we comply with the industry standards that matter most.

HelloSign is compliant with the following standards and regulations:

- SOC 2 Type II
- ISO 27001 including ISO 27018 subset of controls
- Support for HIPPA implementation using the HelloSign and HelloWorks product
- The U.S. ESIGN act of 2000
- The Uniform Electronic Transactions Act (EUTA) of 1999
- The new eIDAS regulation for the EU of 2016 (EU Regulation 910/2014), which replaces the former
- European EC/1999/93 Directive

- EU GDPR (General Data Protection Regulation)

Please contact our security team (via email: security@hellosign.com) for access to our policies, procedures, audits, and assessments which include a copy of our system boundary.

LINKS TO IMPORTANT RESOURCES

Below, you will find additional links to important resources.

HelloSign Terms of Service	**HelloSign Privacy Policy**
HelloSign Trust Center	**Statement of Legality**

02.25.21