docusign

Docusign Trust and Security Overview

eBook

Security has become an integral part of business operations for organizations of all sizes and industries. As ransomware, data breaches and other cyberattacks continue to increase, CIOs consistently rank security and risk management among their top priorities. A robust information security program helps safeguard and protect your customers by weaving comprehensive security measures throughout your technology environment, physical space and business processes. And that's especially true when it comes to confidential documents, contracts and electronic signatures.

When transactions contain highly sensitive information like personally identifiable information, pricing details, proprietary business terms, intellectual property and more, you can't afford to take risks. That's why Docusign emphasizes security and high availability in everything that we do.

For Docusign, security is more than just a competitive differentiator. It's an expression of our key corporate value of trust, and our commitment to operate with integrity, empathy and respect. We care about your business, and we honor the trust you place in our solutions. We fulfill that responsibility with a comprehensive approach addressing the security, privacy, compliance, and validity of your Docusign transactions.

Our approach to security is a big reason why Docusign is the most widely used e-signature solution in the world. Docusign consistently meets the stringent security requirements of even the most security-conscious organizations, including Fortune 500 companies, the world's largest financial institutions, the U.S. Federal Government and other global organizations.

In the following pages, we provide an overview of the Docusign Trust and Security program, including the people, processes, and platform that deliver it, and the certifications and tests that ensure its effectiveness for your business.

Docusign physical safety and security policies



Our dedication to delivering the highest level of security possible for our customers is centered on our Trust and Security Program program, which aligns our people, processes and platform to address the overall security, privacy and validity of your eSignature transactions.

People

Security at Docusign is everyone's job. We invest in training and awareness to ensure that security stays top of mind for all of our employees.

- A cross-functional team of experts who are 100% dedicated to security-related activities
- A centralized repository of security policies, standards, and procedures that's available at all times to groups and individuals throughout our business
- Background checks for all prospective employees and suppliers
- A dedicated Chief Information Security Officer (CISO) who manages security strategy and operations and continuously engages with the security community to ensure Docusign stays ahead of emerging trends in the dynamic threat landscape
- Specialized training for all technical employees to ensure that coding is done securely, with regular security audits of the code base
- Human risk and employee resiliency programs ensure that all employees understand their responsibility to protect customer data and know how to do it
- Annual companywide cybersecurity training addressing privileged access, social engineering, phishing awareness, insider threats, data security, security incident reporting, and more
- Close alignment and collaboration between our governance team and our product design, product maintenance, and support units

Docusign physical safety and security policies



Process

All of Docusign's business processes, including internal policies, software development and platform monitoring, are designed to prioritize the security of our customer data.

- On-premises security policies, such as badge access, manned public entrances and physical access controls
- System access is limited to a minimal number of employees based on the least-privilege principle, with multiple layers of secured authentication required for all critical systems
- Active monitoring and alerting
- Security reviews within the Docusign Software Development Life Cycle (SDLC), including the planning, design, implementation testing, shipping and response phases
- Formal code reviews and vulnerability mitigation by third parties for applications and access security
- Testing and validation of Docusign's key management and encryption program by external auditors and documented in our SSAE 18, SOC1, Type 2 and AT-C 205, SOC2 Type 2 reports

Docusign physical safety and security policies



Platform

Docusign's secure platform encompasses hardware and infrastructure, systems and operations, applications and access, and transmission and storage.

- Commercial-grade data centers with diversity across vendors, so that critical customer documents remain available in the event of any business disruption
- World-class architecture featuring simultaneously active and redundant systems that allow the overall system to survive full-site outages and be "always on"
- A unified control framework to map our security controls to our security certification and compliance responsibilities
- Secure, near real-time data replication
- Physically and logically separated networks for systems and operations
- Malware protection
- Commercial-grade firewalls and border routers to resist/detect IP-based and denial-of-service attacks
- Multiple authentication options for signers
- Anti-tampering controls
- Digital certificate technology
- Two-factor encrypted VPN access

Docusign physical safety and security policies

A holistic approach

Docusign doesn't look at security in a vacuum. We consider all areas that keep your sensitive transactions protected, including privacy and compliance with laws and regulations globally. Docusign's features ensure the enforceability and nonrepudiation of our customers' documents. The following security controls apply to all Docusign products unless otherwise noted.

- AES 256-bit encryption at the application level for customer documents to ensure confidentiality
- Access and transfer of data to/from Docusign via HTTPS
- Use of Security Assertion Markup Language (SAML), giving users the latest capabilities for Web-based authentication and authorization, including single sign-on
- The ability for signers to authenticate when they sign, including multifactor and two-factor authentication
- A digital checksum (mathematical hash value) that validates documents haven't been tampered with outside of each signing event
- Certificates of completion after all parties have participated in the signing process
- Signature verification and unalterable capture of signing parties' names, emails, public IP addresses, signing events, timestamps, signing location (if provided) and completion status
- A digital audit trail for every envelope that captures the name, email address, authentication method, public IP address, envelope action and timestamp[1]

Security certifications

Docusign makes significant investments in enterprise security and operations, and we undergo rigorous scrutiny by third-party auditors to assess and validate the security measures we have in place.

- Consistently meets national and international security standards
- Continual leadership in defining industry best practices for third-party audits, certifications and onsite customer reviews
- Compliance with applicable laws, regulations and industry standards around the world, governing digital transactions and electronic signatures
- Dedicated chief legal officer and chief technology officer that ensure Docusign and our products align with the latest legal and technology trends
- Ability to comply with specialized industry regulations, such

Certifications



ISO 27001:2022

The highest level of global information security assurance available today, ISO 27001 provides customers assurance that Docusign meets stringent international standards on security. Docusign is ISO 27001, 27017, and 27018 certified as an information security management system.[2]
Learn more



APEC PRP

Docusign eSignature has achieved the Asia-Pacific Economic Cooperation (APEC) Privacy Recognition for Processor (PRP) System certification. APEC has established Cross-Border Privacy Rules (CBPR) and Framework to protect the privacy and security of personal information at rest and in transit. An independent auditor, Schellman Group, has assessed our capabilities and granted us this certification to demonstrate compliance with CBPR and Framework.
Learn more



CSA STAR Program

Docusign adheres to the requirements of the Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) program. The CSA STAR comprises key principles of transparency, rigorous auditing and harmonization of standards. Our Consensus Assessments Initiative Questionnaire (CAIQ) documents the rigor and strength of Docusign's security posture and best practices and is publicly accessible for viewing and download from the **CSA STAR registry.**
Learn more



SIG

The SIG (Standardized Information Gathering) Questionnaire is a third-party risk assessment curated by the practitioner members of Shared Assessments. The SIG enables Docusign to annually leverage an industry-standard library of vetted questions measuring risk across 21 domains. It serves as a comprehensive tool for gathering data on security controls, policies, and procedures; providing a standardized method to decrease risk in third-party interactions as well as to increase assessment efficiency for our customers.
Learn more

Certifications

PCI DSS

Docusign maintains compliance with the current version of the PCI Data Security Standard (DSS) to ensure safe and secure handling of credit card holder information. As overseen by the Payment Card Industry Security Standards Council (PCI SSC), Docusign places stringent controls around cardholder data as both a service provider and merchant. Docusign is listed as a PCI Service Provider on the Visa **Global Registry of Services Providers**.
Learn more

SOC 1 Type II and SOC 2 Type II

As a SOC 1 and SOC 2-certified organization, Docusign complies with the reporting requirements stipulated by the American Institute of Certified Public Accountants (AICPA). We undergo yearly audits across our production operations, including our data center, and have sustained and surpassed requirements.
Learn more

Binding Corporate Rules

Docusign obtained approval of its applications for **Binding Corporate Rules** (BCRs) as both a data processor and data controller from the European Union Data Protection Authorities. Docusign's approved BCRs enable lawful cross-border transfers of data through the Docusign platform and eSignature service. Customers will be able to transact business with increased confidence knowing that they will comply with GDPR data transfer requirements when using Docusign.
Learn more

Cloud Computing Compliance Controls Catalog (C5)

C5 Type II compliance validates Docusign's eSignature product security program and controls meet the requirements of the Federal Office for Information Security (BSI). C5 evaluates the security and compliance of cloud service providers operating within the DACH region, considering the unique challenges of cloud computing and creating more transparency about information security and data protection.
Learn more

EU Trusted List

Docusign France SAS, a Docusign company, is a trust service provider (TSP) under EU Regulation 910/214 for electronic identification and trust services (eIDAS). As a TSP, Docusign France provides qualified electronic signatures (QES), qualified time stamps, advanced electronic signatures (AES), and advanced seals recognized by all EU member states. Docusign France is listed as a qualified TSP in the **Trusted List** managed by the French IT Security Agency, ANSSI.
Learn more

FedRAMP (US Federal Risk and Authorization Management Program)

Docusign is listed on the U.S. Federal Government's FedRAMP marketplace with a **Government Cloud deployment model for Docusign eSignature** and a **Public Cloud deployment model for Docusign Contract Lifecycle Management**. Docusign holds a FedRAMP Agency authorization certifying that we follow its standardized approach for assessing, monitoring, and authorizing cloud computing products and services.
Learn more

StateRAMP

StateRAMP establishes common security criteria to standardize cloud security verification. Docusign Federal (eSignature) and Docusign CLM have achieved StateRAMP authorization.
Learn more

Department of Defense Impact Level (IL) 4

According to the DoD CC SRG, DoD IL4 accommodates non-public, unclassified data where the unauthorized disclosure of information could be expected to have a severe, adverse effect on organizational operations and assets, or individuals. Defense Information Systems Agency (DISA) granted Docusign an IL4 provisional authorization for several offerings, including Docusign Federal (eSignature) and Docusign Contract Lifecycle Management.
Learn more

Compilation of (EU) Member States Notification on SSCDs and QSCDs

This publication lists the signature devices that shall be considered as Qualified Signature Creation Devices (QSCDs) under the eIDAS regulation. Docusign owns and operates two remote signature devices, which are listed in the publication, and is the leading global eSignature solution offering cloud-based eIDAS-compliant electronic signatures.
Learn more

Information Security Registered Assessors Program (IRAP)

The Information Security Registered Assessors Program (IRAP) is an Australian Signals Directorate (ASD) initiative to outline a cyber security and risk management framework that organizations can apply to protect Australian government data and systems from cyber threats. Docusign eSignature has been assessed at the Protected Level of control requirements, in alignment with the relevant Australian Government Information Security Manual (ISM) controls and the Protective Security Policy Framework (PSPF).
Learn more

FISC

The Center for Financial Industry Information Systems (FISC) develops security guidelines for information systems, which are followed by most financial institutions in Japan. These include guidelines for security measures to be put in place while creating system architectures, auditing of computer system controls, contingency planning, and developing security policies and procedures. Although compliance with the FISC Security Guidelines is not required by regulation nor audited by FISC, Docusign elected to become a member of the FISC and implemented internal controls to be compliant with the FISC Security Guidelines.
Learn more

Government of Canada Protected-B Program

The Government of Canada Protected-B Program offers a certification framework for Software as a Service (SaaS) companies operating in Canada, ensuring that their software meets stringent security standards necessary for handling sensitive government data at the Protected-B classification level. Docusign has completed thorough assessments, evaluation processes, and personnel security clearance validation to achieve and maintain this certification on a per-department basis.
Learn more



We're committed to fiercely protecting the data our customers entrust to us.

It's why we weave security into every aspect of our organization through the trust and security program, focusing on people, processes and platform. This is evidenced by our investment in meeting national and international security standards, including certification for ISO 27001:2013.

Our customers demand and expect thorough protection of their most sensitive transactions, and that's the stance we take in delivering exceptional document and data security. It's our priority, and it's at the core of every Docusign solution, including Docusign eSignature—the world's number one way to sign electronically on practically any device, from almost anywhere, at any time.

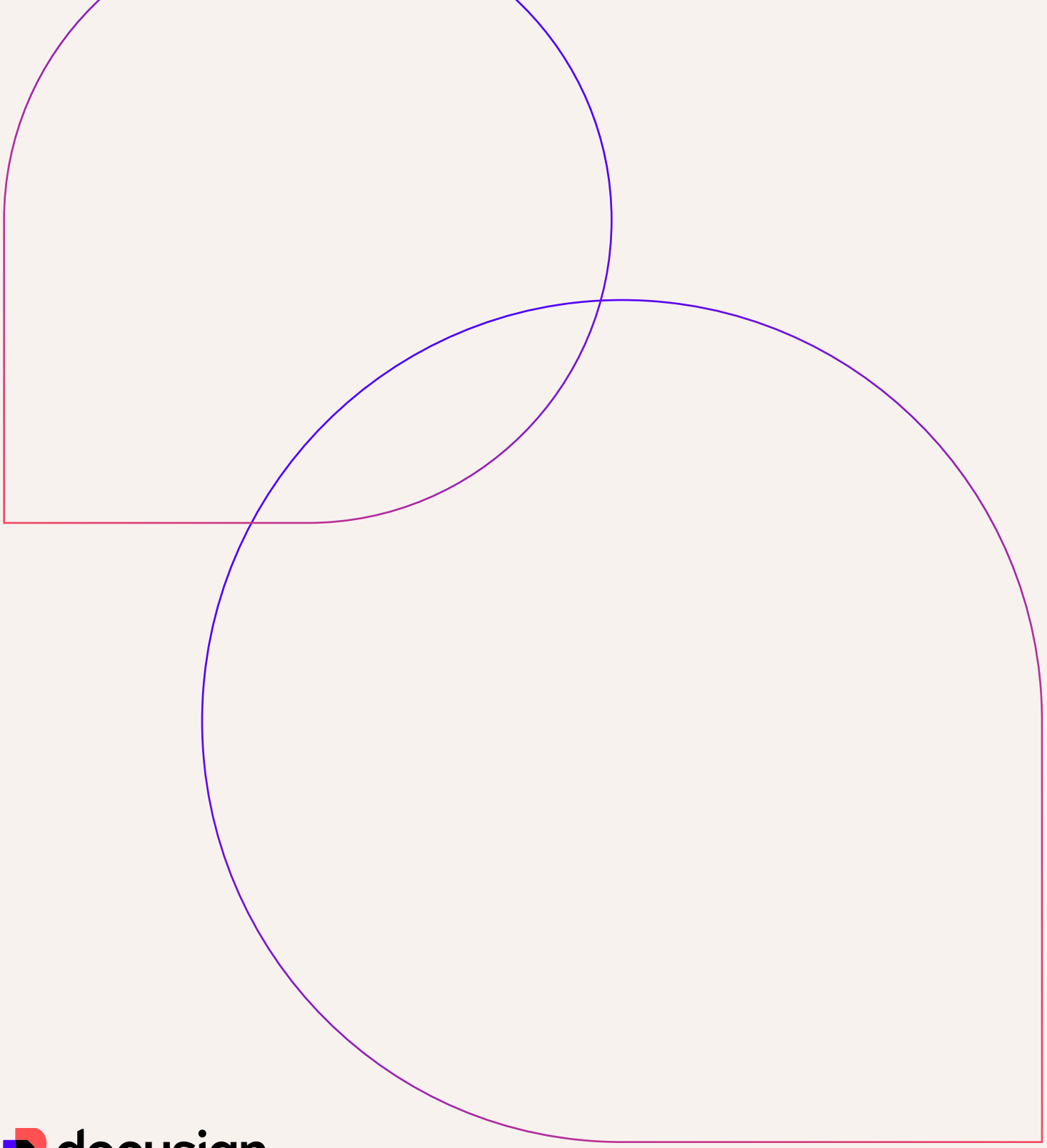
Additional resources

Follow the links below for more details on how we approach and deliver security.

Trust Center
Terms of Use Privacy Policy
Use of Cookies

1 Docusign CLM supports a rich audit trail that is tied to every document in the system. Known as the "History" feature, the audit trail allows users to review a variety of document actions. Full document details and history are captured on every document for its lifetime. Docusign CLM's audit trail automatically captures all changes over the course of the contract lifecycle, including metadata changes, versions, approvals, signing activity, and more. Downloads, comments, automated actions, and more are tracked in the audit trail. All actions recorded in the audit trail feature are tied back to an individual user with time and date stamps. The system tracks document and user activity when contracts are sent for review and editing. Users can see at a glance where all documents are in the process, for example, if they have been sent for editing. If a user has downloaded a document for offline editing it will be recorded in the audit trail and therefore can be reported on.

2 Docusign Notary and Docusign Insight are not certified for ISO 27001:2013



docusign

About Docusign

Docusign brings agreements to life. Over 1.5 million customers and more than a billion people in over 180 countries use Docusign solutions to accelerate the process of doing business and simplify people's lives. With intelligent agreement management, Docusign unleashes business-critical data that is trapped inside of documents. Until now, these were disconnected from business systems of record, costing businesses time, money, and opportunity. Using Docusign IAM, companies can create, commit, and manage agreements with solutions created by the #1 company in e-signature and contract lifecycle management (CLM).

Docusign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105
docusign.com

For more information
sales@docusign.com
+1-877-720-2040