LifeWORKS
A nonprofit serving
people with disabilities

DocuSign Security – Frequently Asked Questions (FAQ)

Introduction

DocuSign is built with comprehensive security from start to finish. This foundation delivers end-to-end security to their customers and their data:

- Confidentiality: customer information stays confidential, including from DocuSign—customer documents and data are private and access is workflow controlled
- Integrity: each document is ensured to be both intact and tamper evident
- Availability: DocuSign's replicated geo-dispersed infrastructure delivers consistent high availability, providing assurance that the service is there whenever customers need it
- Authenticity: customers can rely on the authenticity of signers through the multi-faceted verification of signing events
- Non-repudiation: customer documents are ensured technically and legally and are procedurally unassailable as evidenced by the audit trail and chain of custody available within the DocuSign solution

Frequently Asked Questions

- Are electronic signatures safe?

  Yes, electronic signatures are safe. DocuSign states that an e-signature is more secure that a traditional wet signature. Wet signatures can easily be forged, copied, or tampered with, while electronic signatures have many layers of security and authentication built into them, along with court-admissible proof of transaction.

- How does DocuSign manage security?

  DocuSign eSignature is researched, designed, and developed with security as a top priority. For security details common to all DocuSign products, visit product security on the DocuSign Trust Center: https://www.docusign.com/trust.

- How does DocuSign guarantee data privacy?

  Protecting customer data privacy continues to be a top priority for DocuSign. As new technologies collect increasing amounts of personal data, DocuSign understands the importance of protecting the critical business and personal information entrusted to the DocuSign service.

- How does DocuSign keep data safe?

  To ensure your data stays protected, DocuSign follows industry best practices to:
  - Logically separate individual customer data
  - Encrypt customer data – all data access and transfer activities use HTTPS and other secure protocols, such as SSL, SSH, IPsec, SFTP, or secure channel signing and sealing
  - Support only recognized cipher suites
  - Encrypt all documents with AES 256-bit encryption or the most recent approved methods
  - Provide non-repudiation for all documents generated and signed using DocuSign via a FIPS-Certificate of Completion
  - Maintain a data disposal and re-use policy for managing data assets
  - Implement processes for equipment management and secure media disposal

Resources

All of the information in this document was sourced from the DocuSign Trust Center: https://www.docusign.com/trust. Please visit the Trust Center for more information.

LifeWORKS
A nonprofit serving
people with disabilities

Version No	1.0	Status	Final
Author	Don Becchetti	Revision Date	05-14-2021
Approver/Owner	Don Becchetti	Approval Date	05-25-2021