Documoto Security

Securing Your Most Valuable Assets

The Documoto Data Center

Documoto is provided under a SaaS (Software as a Service) deployment model, with the infrastructure and data residing entirely at Amazon Web Services (AWS) in Northern Virginia, US. Most Documoto components, including all persistent data storage, is inaccessible to the internet at large. As an AWS customer, while we take advantage of the leading compliance and security features offered by AWS, security is a shared responsibility between Documoto (our application, its architecture and infrastructure configuration, access management, our internal security practices, and so on), our customers (authentication schemes, policies and procedures, I/T security, and so on), and AWS (SSAE 16 standards, compliance audits, physical security, and so on).

AWS is a world-class provider of cloud-based services and infrastructure with robust physical security, frequent 3rd party audits, and various tools and utilities to identify and resolve security issues. As our data center, they certify compliance under SSAE 16/ISAE 3402, including SOC 1, SOC 2 Type I and II, and SOC 3 reports. They also certify compliance under ISO/IEC 27001:2013, 27017:2015, and 27018:2019.

Facility Security

- Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means.
- Physical access points to server rooms are recorded by Closed Circuit Television Camera.
- Authorized staff utilize multi-factor authentication mechanisms to access data centers.

Facility Design

- 24 x 7 x 365 fully staffed Network Operations Center.
- Redundant network carriers.
- Automatic fire detection and suppression equipment.
- Systems monitor and control temperature and humidity at appropriate levels.

Facility Power

- Data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day.
- All data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

Documoto Security

Securing Your Most Valuable Assets

AWS Security Processes

AWS maintains compliance under SSAE 16 / ISAE 3402, including SOC 1, SOC 2, SOC 2 Type 1, and SOC 3. AWS System and Organization Controls (SOC) Reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help you and your auditors understand the AWS controls established to support operations and compliance (https://aws.amazon.com/compliance/soc-faqs/).

- AWS SOC 1 Report.
- AWS SOC 2 Security, Availability & Confidentiality Report.
- AWS SOC 2 Security, Availability & Confidentiality Report.
- AWS SOC 2 Privacy Type I Report.
- AWS SOC 3 Security, Availability & Confidentiality Report, publicly available as a whitepaper.

For further information, see the AWS Security Whitepaper here: https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Communication & Operating Systems Security

We write our software taking into account modern security breach exploitations used in the Internet including cross-site scripting, JavaScript and SQL injections.

Taking this a step further, all communication between a client PC and our servers is secured via Secure Sockets Layer (SSL). This is a cryptographic protocol that provides communications security over the Internet, designed to prevent eavesdropping and tampering of data. In addition, we validate each session, greatly reducing the possibility of session hijacking.

Access to the Documoto production system is strictly enforced via the principle of "least privilege," giving access to the network to only those who need it and with only powers which are absolutely essential to do his/her work.

Documoto servers are hardened based on the latest best practices. We perform vulnerability assessments regularly. Exceptions are remedied as appropriate. Operating system and Documoto code patches are installed during scheduled maintenance windows. All patches are reviewed before being applied to the production environment.

Documoto Security

Securing Your Most Valuable Assets

Objects & Data Security in a Multi-Tenant Environment

"Multi-tenant" and "Cloud" are phrases often heard in today's software world. In the most basic form, they mean multiple customers sharing one physical instance of a software platform, without ever seeing each other's application data.

We engineered Documoto as a secured multi-tenant system from the ground up, developing virtual security walls between each Documoto tenant. Each tenant is given a Tenant Encrypted Key (TEK) which serves as a digital gateway to only their data.

When users are created, they are associated with only one tenant. As they log into the system, our application stack ensures the data returned is from the same tenant to which the user belongs.

Furthermore, our security model allows for very granular information access and privileges. You control who in your organization has access to which documents by separating them into "user groups" with unique access controls.

In addition, no keys, passwords or other security information are stored on the client PC.

All keys and passwords are digitally encrypted on the server using the latest one-way cryptography technology. This means that not even Documoto staff has the ability to decode a password for security reasons.

Documents are vaulted, ensuring they cannot be accessed without logging into the system and they can never be retrieved directly by typing a URL into the browser. With our secured application layer, there is no way for any user in a tenant to access the information or documents of another tenant production environment.

Data Privacy & GDPR

Documoto respects our customer's privacy. We do not sell or disclose your information to 3rd parties. Further, we adhere to a published privacy policy and are compliant with GDPR (General Data Protection Regulation) as both a processor and a controller, as applicable.

Rest assured, your data is always secure!