DocsCorp

DocsCorp cloud – Information Security

At DocsCorp, the security of your data is our highest priority. Our highly-experienced development team incorporates security requirements from the earliest possible opportunity and continues to address security requirements at every development phase, from initial planning to releases and updates. DocsCorp uses the best tools and engineering practices available to build and maintain DocsCorp cloud.

DocsCorp cloud is designed with multiple layers of protection, including secure data transfer, encryption, and application and user-level controls that are distributed across a highly scalable and secure infrastructure, provided by Microsoft Azure. Read more about Microsoft Azure security - www.microsoft.com/en-us/trustcenter/security/azure-security

Learn More

- DocsCorp cloud performs most operations on your files using volatile memory (e.g. Random-access memory, RAM) rather than non-volatile memory (e.g. flash, disk or attached storage); reducing the need for your files to be at rest.

- DocsCorp cloud files may be at rest for a short period of time to support the DocsCorp cloud applications and services we provide to you. Files at rest are automatically removed when no longer required.

- DocsCorp cloud files are encrypted using user-specific 256-bit Advanced Encryption Standard (AES) keys which are in turn protected by a secure key management service (Azure Key Vault); it is designed to segregate/partition user data in a multi-tenant architecture and to ensure the privacy of your data between users of your tenancy and DocsCorp cloud.

- DocsCorp cloud only sees non-identifying data around documents uploaded to the service e.g. document identifiers, never document titles or metadata within the document itself. Some profile metadata is retained for a short time to facilitate saving of processed documents back into the DMS. No personally identifiable information (PII) is accessed or retained in the system.

- DocsCorp cloud uses Transport Layer Security (TLS) to protect data in transit between DocsCorp cloud apps and our servers; it is designed to create a secure tunnel protected by 256-bit or higher encryption.

DocsCorp
Work smart

- DocsCorp cloud apps, servers and infrastructure are regularly tested for security vulnerabilities and hardened to enhance security and protect against attacks.

- DocsCorp cloud provides secure access only via well-known trusted single sign-on (SSO) OAuth2 providers (e.g. Azure Active Directory and Microsoft accounts); designed to leverage existing Identity Directory Providers (IdP) whereby users or administrators may implement two-factor authentication (2FA) for an extra layer of protection at sign-on.

- DocsCorp employees and other DocsCorp cloud users cannot see your files sent to our services. Your files are protected by secure data transfer, encryption, and application and user-level controls. In the rare occurrence, like most online services, we have a small number of engineering and support personnel who may request access to your data on a one-time basis to support your experience using our service. In most cases, any documents that may be requested to provide support can be provided by you to DocsCorp outside of the DocsCorp cloud i.e. no access needed in the cloud system. If any access within the system was required, your explicit permission is required to grant access and all access is logged and audited. Under no other circumstance will access to your data be permitted.

- DocsCorp cloud is hosted on Azure and developed with development tools from Microsoft, an ISO/IEC 27001 accredited organization. To meet your data protection requirements data can be domiciled in the US, Netherlands, or Australia.

SYDNEY
LONDON
PITTSBURGH

E: info@docscorp.com
P: +61 (0)2 8270 8500

www.docscorp.com