1DocStop
One Stop Document Management

CLOUD SECURITY

FEATURES

- Files stored in Microsoft's Ultra-Secure Tier-1 Data
- Centers co-located within the United States
- HIPAA Compliant Security
- Client/Server protected with 256-bit encryption
- Passwords stored as hash and cannot be recovered

1DOCSTOP STORAGE SECURITY

SyTech's 1DocStop platform runs exclusively on Microsoft's Windows Azure Cloud. Files are stored and co-located in Microsoft's Ultra-Secure Tier-1 Data Centers.

1DocStop's data layer consists of native Azure storage technology including Table, Queue, and Blob storage. The data layer is accessed exclusively through user-authenticated ASP.NET WCF web services.

PORTAL SECURITY

Access to 1DocStop and its respective services are secured using industry standard protocols adopted to protect Hf PAA-Class document storage.

All communication between services and client browser/application/mobile device(s) are protected by 256-bit transport layer security secured using verified SSL certificates.

AUTHENTICATION

Credentials are comprised of an email address and a user-defined password. SyTech's support staff will NEVER ask a user for their password.

All password information is hashed and encrypted using a one-way string encryption before storage. Passwords cannot be recovered from the database and so requires a complete reset should a user forget his or her password.

TRANSPORT LAYER SECURITY

All 1DocStop service communications are secured using transport layer security. This is the go-to standard practice for all sensitive services available online. It involves both the browser and the server encrypting the packets before they are transported over the internet. These packets are only readable once they have been received by their authorized recipients.

Any communication intercepted between the browser and the service is encrypted using 256-bit keys and therefore useless to an unauthorized party.

www.sytechsolutions.com