Security Overview

SyTech staff adheres to strict confidentiality standards and undergoes a regular training program to ensure that the highest industry standards are met—including security training and review for the Health Insurance Portability and Accountability Act (HIPPA), California State law, Federal law, and the Sarbanes Oxley Act (SOX). We consistently work with confidential information and have the proper security and standards in place. All of SyTech's employees have executed confidentiality agreements that protect the documents of third parties. Located next to the Elk Grove Police Department, our secure production facility is protected with restricted access, 24/hour surveillance, biometric locks, and access is restricted to employees only.

- BUILDING: SyTech's stand-alone production facility is not shared with any other tenant. SyTech hired a consultant who designs security systems for banks to help design our production facility. Our building was designed and constructed specifically with record and data security in mind. All exterior doors and windows (windows are located only in the lobby area) are hard wired with alarms. Access to all entry points into and within the production facility is protected by electronic access control mechanisms which allow only authorized individuals to enter the production area. Furthermore, the IT area is also protected with its separate biometric fingerprint readers. SyTech's facility has 16 security cameras in place throughout all critical areas, both inside and out of our building.

- SHREDDING: Upon approval, records are shredded on-site in a manner that exceeds DoD standards. Cameras are connected to the shredders so you can actually watch the records as they are being destroyed and destruction certificates provided.

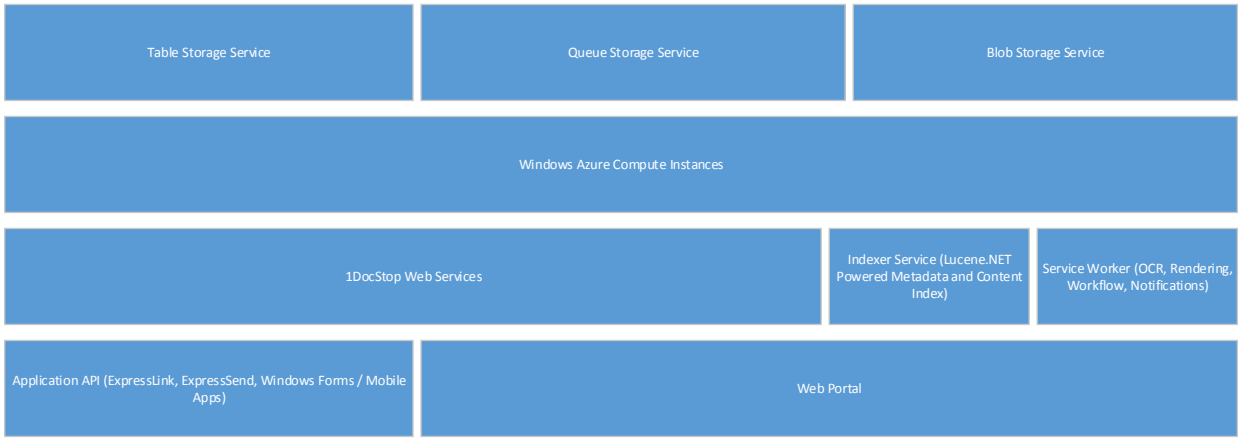
- TRANSPORTATION: Although it has never been required, in case of emergency, our vehicles are equipped with hidden transponder devices that, when enabled, show the GPS coordinates of the vehicle to protect records during transport and to assist police in its recovery.

- DATA MONITORING: SyTech provides daily monitoring of its hosting network to ensure uptime and identify possible security issues. Current security management includes monitoring of both application and IIS access logs, server to client communications encryption using secure server certificates (128-bit), and user password encryption.

- INSURANCE: In addition to General Liability Insurance, Professional Liability Insurance, Workers' Compensation Insurance and Auto Insurance policies, SyTech also has a specific rider on its E&O policy that covers network security and data privacy. SyTech will name you as an Additional Insured on its policies upon request.

Storage Security

The 1DocStop document platform runs exclusively on Microsoft's Windows Azure Cloud. 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.



Table

The Windows Azure Table storage service stores large amounts of structured data. The service is a NoSQL datastore which accepts authenticated calls from inside and outside the Windows Azure cloud. Windows Azure tables are ideal for storing structured, non-relational data. Common uses of the Table service include:

- Storing TBs of structured data capable of serving web scale applications
- Storing datasets that don't require complex joins, foreign keys, or stored procedures and can be de-normalized for fast access
- Quickly querying data using a clustered index
- Accessing data using the OData protocol and LINQ queries with WCF Data Service .NET Libraries

1DocStop stores all document metadata, system data, and log info in Azure Table Storage.

Queue

Windows Azure Queue storage is a service for storing large numbers of messages that can be accessed from anywhere in the world via authenticated calls using HTTP or HTTPS. A single queue message can be up to 64KB in size, a queue can contain millions of messages, up to the 100TB total capacity limit of a storage account. Common uses of Queue storage include:

- Creating a backlog of work to process asynchronously
- Passing messages from a Windows Azure Web role to a Windows Azure Worker role

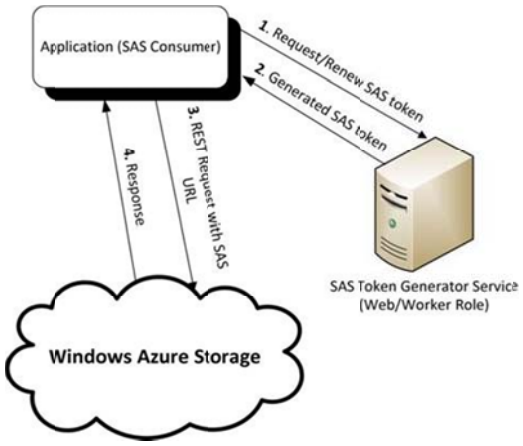
1DocStop uses Azure Queue Storage to manage long running tasks such as content indexing and preview/thumbnail rendering.

Blob

Windows Azure Blob storage is a service for storing large amounts of unstructured data that can be accessed from anywhere in the world via HTTP or HTTPS. A single blob can be hundreds of gigabytes in size, and a single storage account can contain up to 100TB of blobs. Common uses of Blob storage include:

- Serving images or documents directly to a browser
- Storing files for distributed access
- Streaming video and audio
- Performing secure backup and disaster recovery
- Storing data for analysis by an on-premises or Windows Azure-hosted service

Blob storage is used by the 1DocStop platform to store all document files. All access to the blob storage service is secured through the use of Shared Access Signatures.



A Shared Access Signature is an expiring key providing lease access to the key holder. Shared Access Signatures are specific to an individual blob item and must be generated at runtime. SAS tokens are only valid for 45 minutes after they are requested for writes and 10 minutes for reads.

Portal Security

All access to 1DocStop and its respective services are secured using industry standard protocols adopted to protect HIPPA class document storage. All communication between services and client browser/application/mobile device is protected by 128-bit transport layer security secured using verified SSL certificates.

Authentication

Every request to the 1DocStop platform requires either a valid authenticated token or a valid set of credentials. Credentials are comprised of an email address and a user defined password. SyTech support staff will never ask a user for their password and all password information is hashed and encrypted using a one-way string encryption before being stored. A password cannot be recovered from database and so requires a complete reset should the user forget their password.

To reduce login fatigue, an authentication token is created on successful login. This token includes certain localized entropy such as IP, browser version, date-time offset, etc. to create a security token that can be used in place of a credential set. This token is only valid for the current session and invalidated immediately if any of entropy points are modified.

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. They are only readable once they have been received by the respective recipients. Any communication intercepted between the browser and the service would be encrypted using a 128-bit key and therefore useless.

Physical Security

These specific procedures will be undertaken with your project to ensure that mission-critical records receive the highest possible protection available. The security plan that we have put in place will ensure the security of all records to prevent their damage or destruction and to also ensure their confidentiality. SyTech has identified the greatest threat to your confidential mission critical records, and the best solution to mitigate that risk. The chart below identifies how we will protect the records from pickup to ultimate disposal:

Secure Daily Transport	• Drivers equipped with GPS tracking devices. • Van will be securely locked at all times and no stops will be made by drivers between trips from and SyTech and your facility. • Backup Drivers in place to ensure daily pickup prior to 10:00 am. • Flawless 12 year track record of daily pickups and processing of critical records from other clients and state agencies.
Secure Facility	• All records will be processed at SyTech's secure Elk Grove Facility, located next to the Elk Grove Police Department. • Biometric security prevents access past reception area. Visitors must be accompanied by an employee. • Access monitored 24/7 by security system and cameras. • Stand-alone building not shared with other tenants.

	• Independent monitoring of fire and alarm systems. • Alarm system equipped with cellular backup. • Building staffed day and swing shift. • Comprehensive closing checklist signed off by the swing shift supervisor on nightly basis. • Building in unoccupied only 7.5 hours/day, during which facility is further protected by 24 hour security cameras and alarm.
Biometric Secured Project Processing Room	• Records will be immediately logged and placed for immediate processing in an area dedicated for sensitive projects. • The room is protected by additional biometric security locks, accessible only by supervisors and authorized employees. • All records will be physically stored in this room until their scanned images have been backed up at a Tier 1, Azure data center. • Boxes will be catalogued by date and internal tracking system for expeditious handling of physical record requests detailed in the Record Retention section below.
Daily Scanning & Backup of Forms	• All records will be scanned and backed up on a daily basis. • SyTech will utilize Kofax with VRS to ensure the best possible image quality of the record is obtained during the scanning process.
Azure, Tier 1 Data Center Backup	• Weekly backups of all forms will be stored at Microsoft (Tier 1) Data Center, mirrored in Nevada (described more fully below). • Images will be stored in non-proprietary Group IV TIFF images. • SyTech will also provide client with backups of the images as requested.
Flood Protection—Above 100 Year Plain	• Location of building is above Sacramento 100 year flood plain.
"Chain-Of-Custody" (COC) Documentation & Real Time Tracking	• SyTech will adhere to client "Chain-Of-Custody" (COC) documentation and tracking requirements. • Chain of Custody managed by Project Manager, Jonathan Pritt a licensed California Attorney. • Only those employees authorized to work on this project will have access to those records. • During the performance of this contract, authorized personnel will tracks the location of all projects. This will also allow for rapid handling of record requests. At the conclusion of the contract, a record containing all Chain-of-Custody documentation can be provided if requested.

Audit of Physical Security Plan	• SyTech performs routine audits of our security plan.
Employee Screening & Best PracticeTraining	• SyTech employees have extensive experience working with highly sensitive confidential records (including Alameda County Sheriff Dept., Sacramento County Sheriff Dept., S.F. and San Mateo County Bureau of Environmental Health, and the California Dept. of Health Service). • SyTech's building does not allow access to non-employees beyond the reception area (biometric doors). • SyTech provides continual best practice training to its employees to protect sensitive records it processes for its clients.
Confidentiality Agreements	• All SyTech employees have executed a comprehensive Confidentiality Agreements. These are available upon request.
Document Destruction	• Destruction will be followed per the written instructions, and in the manner proscribed by the Contract Manager. • Records designated for further retention beyond that specified in the retention schedule (such as those pertaining to pending litigation) will not be destroyed. • Physical records will be destroyed on-site (not removed off-site unless directed by client). • Client personnel are welcome to witness the destruction of their files if desired. • Verification of destruction forms will be completed documenting all records destroyed.

Privacy

SyTech has worked with hundreds of public customers and takes privacy very seriously. The majority of our client base is public agencies responsible for storing confidential information for extremely long periods of time. These agencies are tasked with the storage and retrieval of documents ranging from publicly available board minutes to HIPPA classified medical records. We have been providing document management services for many of these customers for more than a decade.

The documents and associated metadata that we store for our customers is always treated as the respective customer's private property. It is never aggregated, sold, or provided to third parties for any purpose. We work with each customer to ensure they understand this policy, provide them the tools to restrict access, and store access statistics so that administrators can track each instance a document was accessed.

Group Access Policies

Documents are categorized by schema or property collections called Document Types. These types are used to determine how a document will be stored, searched, and retrieved. Additionally, document types are the smallest unit for controlling access by user group. Each 1DocStop user account can belong to only one group. Each group has an array of document types that its users can access. This keeps access control simple, obvious, and explicit.

Access is defined as one of 4 types.

- Read – Ability to read the document from storage.
- Modify – Ability to change classification of a record as well as change its applied document schema.
- Create – Create allows the group's users to create or add new documents of this schema to the repository.
- Delete – Ability to mark a document for deletion on the next purge cycle.

Access Log

Every time a document stored in 1DocStop is accessed, an access event object is created and stored for that document. This event object includes the date and time of the access, the user account id that accessed it, and the methods that were called on it. This log can be viewed at both the document level and the user level to assist in monitoring the database. Access by SyTech support staff is recorded in the same manner and is reviewable by customer administrators.

SyTech Technician Access

SyTech access is limited by policy to support incidents only. This policy is enforced through review of the access logs and support ticket reconciliation. All SyTech support access is logged in the same manner as customer's user accounts. The nature of Azure Blob storage requires that access to document files include private keys generated by the service. This requirement prevents out of band access to document files stored by the system including access by SyTech's support staff.

Optional Encryption @ Rest

Additionally, customers may request encryption at rest which encrypts each document before storing it to Azure Blob storage. Encryption at rest generates an additional private key specific to the customer for use with an RSA encryption algorithm to obscure the contents of a file before it is stored. This would be an additional layer of protection should Microsoft's blob storage service be compromised. This extra protection comes at a cost to performance as each document must be processed by the encryption services for each access. This can slow the access for larger documents >250 pages or ~15MB. Content indexing and image preview/thumbnail rendering times are also impacted.