# SmartVault Security

At SmartVault, we take the responsibility of protecting your business's sensitive documents very seriously. We've engineered the SmartVault service from the ground up to protect your valuable digital assets.

Our team has over 50 years of combined and diversified experience in dealing with security, privacy, and compliance issues. We take a disciplined approach to protecting your documents. We continually evaluate and seek to improve our security technology and procedures.

For more information about how SmartVault supports your compliance or regulatory needs, such as those associated with HIPPA, GLBA, FINRA, or SEC, please visit our **compliance resource center** at **smartvault.com/compliance**.

For answers to our most frequently asked questions about security, please review our **Security FAQ** at **smartvault.com/security/faq**

Join our on-demand webinar series on cloud security, **Partnering for a More Secure Cloud**, and get practical advice, in everyday terms (we promise no geek-speak here!), designed to help you protect and secure your data in the cloud. **smartvault.com/resource/partnering-for-a-more-secure-cloud-webinar-series**

## Your Data is Secure While in Transit

All interactions with SmartVault occur over an encrypted channel. We employ SSL to protect your documents, passwords, and interactions with SmartVault from eavesdropping.

## Your Data is Secure While at Rest

SmartVault encrypts your documents and all information stored in our databases at rest. The data is encrypted using AES-256. More details can be found in our **Security FAQ** at **smartvault.com/security/faq**

## How Your Data is Stored

SmartVault is designed to allow access to documents via authenticated logins. In other words, documents stored in SmartVault are only accessible if you log into the service or share the documents with another individual that must log into the service. SmartVault employs an Activity Log that you can use to review:

- Who has been granted permissions to access documents
- Who has actually accessed documents

SmartVault classifies the information you store in SmartVault into two categories: *confidential data* and *sensitive data*.

### Confidential Data

Confidential data includes the contents of documents, credit card account number, and password hashes. Confidential information is accessible by a limited number of SmartVault employees; however, SmartVault has processes and technologies which forbid access to that data without your express permission. Staff with this level of access are screened and trained on SmartVault's security controls designed to protect your privacy. Auditing mechanisms are in place to detect any violation of this policy.

SmartVault uses the Payment Card Industry (PCI) Data Security Standard (DSS) as an actionable framework to provide a robust security process. This standard is designed to protect credit card information; however, SmartVault employs this framework as a tool across all confidential information – including your documents. This framework provides us a security process that incorporates prevention, detection, and appropriate response to security incidents.

The PCI Security Standards Council provides more information regarding PCI DSS at **pcisecuritystandards.org/security_standards**

## How Your Data is Stored

*continued*

### Sensitive Data

Information not deemed confidential is considered sensitive. Sensitive information includes your email address, account name, document names, folder names, and other metadata. For this reason, we recommend that you never include confidential information (such as social security numbers, credit card numbers, etc.) in document names, folder names, or description fields. In effect, confidential information should only be included inside an actual document. Sensitive information may be used by SmartVault employees to troubleshoot problems, resolve account management issues, and support marketing efforts. Our staff is trained on the need to protect sensitive information. SmartVault's privacy policy: **smartvault.com/privacy-policy**

SmartVault hosts your data at CyrusOne, in Houston, Texas. CyrusOne has an SSAE 16 Assessment Report. This report is available by sending a request to **support@smartvault.com**. Their facility uses physical barriers, video surveillance, and a professional security staff to keep the data center secure and protected.More information on CyrusOne's security can be found at **cyrusone.com**.

## Your Data is Backed Up

Your documents and metadata are always stored in redundant, replicated storage. After document upload, we store at least 2 copies of your documents. This ensures availability as well as scalability. Further, once a day documents are archived onto offline storage. As with live storage, at least 2 copies exist of your metadata as well as documents. Therefore SmartVault maintains 4 copies of your documents and metadata—2 onsite and 2 offsite to ensure data accessibility and data recover ability.

## Compliance Requirements

At SmartVault, we know that many businesses face compliance pressure when managing sensitive customer information and documents. For more information, please visit our **compliance resource center** at **smartvault.com/compliance**

## Your Role in Protecting Your Assets

Protecting your assets is a team effort between you and SmartVault, and we take this partnership very seriously. As such, we feel it is critical to help you do your part. Security is a tough balance between protection and efficiency. Just as military fortifications are very secure, they are hard to enter and exit. The additional procedures that secure the facility effectively slow down operations within. That being said, we want to provide you guidance on measures that you can take to improve your protection, and still meet your business needs.

Here are some simple steps that every SmartVault user should employ:

- Protect your session by signing out of the service when not in use
- Use good password practices
- Assess your own, unique data protection needs

Good password practices include:

- Using a strong password (lowercase, uppercase, numbers, symbols, etc.)
- Changing your password every 90 days
- Not using the same password you use at other sites or other computers
- Not sharing your password with anyone, including SmartVault employees. (SmartVault employees are never allowed to ask you for your password.)

## Your Role in Protecting Your Assets

*continued*

Further, we encourage our customers to assess their own, individual data protection needs. For example, if you require additional data protection beyond what the SmartVault service provides, you can use third-party encryption systems to encrypt documents before storing them in SmartVault.

## Where Do I Report Security Concerns?

Our top priority is making SmartVault safe for all of our users. While we're very confident in our security technology, we prefer to investigate any and all reported security concerns with any of SmartVault's services or software.

Please report security problems or questions to **security@smartvault.com**