SmartVault Security FAQ

Security is our top priority, and we often get asked questions about our security practices, which we've compiled below. For a more complete guide to our security practices, visit the **SmartVault Security Overview**.

Where is my SmartVault data stored?

SmartVault hosts your data using services provided by Amazon Web Services (AWS) and CyrusOne.

Amazon Web Services are trusted and relied upon all over the world to provide highly secure and scalable infrastructure. Learn more about Amazon Web Services security **here**, including their **System & Organizational Control (SOC) report**.

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. Learn more about CyrusOne's security **here**.

How do I know that my documents stored in SmartVault will always be available? What is the SLA?

The SmartVault Service Level Agreement is 99.9% uptime to ensure anywhere, any time access to your documents.

How often is the data that I store in the SmartVault data center backed up?

SmartVault maintains copies of your files both in its live data center and in offsite archives. Redundant copies of your files are created after you upload a file. Further, archived copies of your files are created within 24 hours after upload. SmartVault can recover files deleted up to 90 days ago. These files can be recovered using the recycle bin feature. Also, most SmartVault plans offer access to unlimited revision history for a file. If you deleted a file more than 90 days ago, please contact SmartVault support — we still may be able to recover your file.

What kinds of password policies do you enforce in SmartVault or can I enforce in SmartVault?

The SmartVault service enforces a strong password policy – passwords must be a minimum of 12 characters in length and must include one of each of the following: upper case letter, lower case letter, number, and punctuation. We recommend that businesses review their password needs and designate a password policy as part of their employee and client on boarding process. Employees and clients should be instructed in proper password handling, selection of appropriate passwords, and procedures for changing passwords in case of password compromise.

The SANS institute has a sample **password policy** that you can use as a primer for developing your own password policy.

Does SmartVault use encryption?

Yes. SmartVault uses SSL when you or others you invite to your SmartVault account interact and communicate with SmartVault by uploading, viewing, and downloading documents. This protects your documents, passwords, and other interactions with SmartVault from eaves-dropping.

SmartVault also encrypts backups of your documents and their metadata, and then stores these encrypted backups offsite. Because of this, any backup media intercepted or lost in transit from SmartVault to the secure, offsite facility is non-recoverable by eavesdroppers.

All documents stored in the SmartVault data center are encrypted at rest using AES-256.

Further, documents at rest in the data center are segregated into a data network designed to protect confidential data. SmartVault uses the Payment Card Industry (PCI) Data Security Standard (DSS) as an actionable framework to provide a robust security process in this environment. 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.

How does SmartVault support the Gramm-Leach-Bliley Act (GLBA)?

SmartVault adds value to your financial services workflow by giving you the ability to store all of your files securely online, access documents when you need them, and safely share files with the right people. It's easy for you to use with features specifically designed for financial service companies to automate workflow and meet compliance mandates.

Although we are not a financial institution, SmartVault has put security processes and protocols in place that make it part of a GLBA compliant solution for financial institutions. Including:

Public privacy policy

- We do not sell or rent your nonpublic personal information or tax information to anyone without your permission.
- We do not share your personal information with anyone outside of SmartVault for promotional and/or marketing use.

SSL encryption for documents in transit
Protecting your documents, passwords and interactions with SmartVault from eavesdropping

SSAE 16 Data Center with Service Auditor's report available

Document access via authenticated login
Files are only accessible to users of the service (no anonymous sharing of files)

Activity Logs
Complete audit history of who accessed and/or modified documents stored in SmartVault

Granular access
Ability to grant access to specific folders

Keep in mind that GLBA compliance is a financial institution obligation, not a technical specification. So when we say that SmartVault supports a GLBA compliant workflow, what we mean is that our service gives you the tools that financial institutions need in order to work in a GLBA-compliant fashion.

How does SmartVault support FINRA compliance?

SmartVault can be part of your company's FINRA compliant solution. Regulation 4370 (c)(1) addresses data backup and recovery of electronic records. Your documents and metadata are always stored in redundant, replicated storage. After document upload, we store at least two 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 two copies exist of your metadata as well as documents. Therefore SmartVault maintains four copies of your documents and metadata — two onsite and two offsite to ensure data accessibility and data recoverability.

How long has SmartVault been in business? What would happen to my documents if SmartVault goes out of business? How would I get my documents back?

SmartVault has been in business since 2008, and today thousands of business and accounting professionals use SmartVault to store and share their business documents securely online.

In the unlikely event of business failure, SmartVault has a plan in place for gracefully transitioning your documents back to you. SmartVault also has business continuity insurance to protect against such an unexpected event.

In addition, you can always create an archive of the documents you have stored in SmartVault on your local computer or on a network drive at any time, on-demand, using the SmartVault Drive. Additional information about how you can create an archive of your SmartVault documents on-demand on your local computer or on a network drive, is available here.

Can storing data on a server in my office be more secure than a cloud solution, especially if I do regular backups and store the backups offsite?

Storing data on a server in your office can be very secure, especially if you have good data security and disaster recover policies and processes in place. However, when determining if you want to store your data on a server in your office or in the cloud, ensure you evaluate the feasibility with regard to skills, cost, and available time to determine if you can realistically provide a more secure and compliant solution. SmartVault uses the **Payment Card Industry (PCI)** Data Security Standard (DSS), as an actionable security framework and strives to exceed the standard requirements. We evaluate our adherence to this standard annually. We encourage you to use this as benchmark to evaluate your own operations if you store documents on-site in your office.

Is SmartVault PCI Compliant?

Yes. SmartVault complies with PCI DSS Level D.

How can I use SmartVault to achieve PCI compliance?

SmartVault can help you cover several aspects of your PCI requirements; especially when combined with publicly available encryption technology. Specifically, we can help you address aspects such as authenticated access and audit trails. Although we are not in the business of providing compliance consultancy, we are happy to get you pointed in the right direction. Feel free to contact us at **security@smartvault.com** for more insight.

Are SmartVault employees bonded?

Yes, all SmartVault employees are covered by employee dishonesty coverage (often referred to as bonded).