



SAS 70 Compliance
Fortress Computer Service, LLC

SAS 70 Compliance

You can trust your data with our company. Whether it's backing up revisions or restoring your files, your data will be there when you need it. Why are we so sure? Our online backup solution is SAS 70 certified.

What is SAS 70?

SAS 70 is an accounting standard developed by the American Institute of Certified Public Accountants. During an audit, a third-party will evaluate a service organization's internal controls and security standards. When an independent auditor conducts the review, they verify that the proper operational controls, procedures, and risk assessments are in place.

SAS 70 audits controls over information technology and processes related to sensitive data, such as health information and personally identifiable information. The audit process is ongoing; third-party evaluations are regularly scheduled to ensure continued compliance.

Why is SAS 70 important?

SAS 70 is recognized as one of the most stringent auditing standards for service organizations. A successful audit verification ensures that the company has well-designed and effective controls in place to ensure the accuracy of transactions and privacy of the data being stored and transmitted.

Organizations, which provide services to healthcare companies, are often asked by their clients to have a SAS 70 audit conducted to ensure that an independent party has examined the controls over the processing of sensitive healthcare information.

A SAS 70 certification is used by customers, prospective customers, and investors to gain an understanding of the control environment of outsourcing companies.

Who is certified?

Not all service providers are SAS 70 certified. With our company, you can be assured that your data is both safe and secure now and in the future.

A First in Data Security Law

The nation's most stringent data security law, the Massachusetts Data Protection Regulation (MA 201 CMR 17), is now in effect. For the first time ever, a government body has mandated the use of a specific technology to enforce privacy regulations. Massachusetts (along with Nevada, who recently passed a similar law) requires that businesses encrypt all the transmitted, personally identifiable information (PII) of their customers.

Not only does this law apply to Massachusetts businesses; it applies to any firm conducting business with any resident of Massachusetts, including third-party vendors. In effect, any company who wants to sell anything to a resident of the nation's 13th largest economy must adopt these measures.

Largest Data Breach in History

These new regulations are being ushered in on the heels of the most significant data breach in history. In 2007, TJX Companies, based in Framingham, Mass., announced a data breach in which hackers exposed at least 45.7 million credit and debit card holders to identity fraud.

TJX has since settled a number of lawsuits and agreed to implement tighter security and obtain independent audits every other year for 20 years, according to a settlement reached with the Federal Trade Commission.

As a result of this catastrophic data loss, this new law was designed to protect consumers on three fronts:

- To insure the security and confidentiality of customer information
- To protect against anticipated threats or hazards to the security or integrity of such information
- To protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer

Beyond Encryption

Yet the Massachusetts law is much more than an encryption mandate. Encryption is only a part of an overall information security plan that businesses must develop. Other computer system requirements include: secure user authentication protocols, secure access control measures, reasonable monitoring of systems, and up-to-date software.

Beyond system requirements, businesses are also accountable for making sure that their human resources can implement and maintain these programs. Business must: 1) designate one or more employees to maintain the security program, 2) provide ongoing employee training, and 3) develop security policies for employees relating to the storage, access, and transportation of records.

However, according to the Commonwealth, these safeguards should be appropriate to the size of the business, the amount of resources available to that business, and the amount of sensitive data stored. Essentially, the law requires businesses to put forth their "best effort" to ensure certain types of data are protected to the best of their ability.

If a public data breach does occur, the application of this law will hinge on the answer to the question, "Did you do everything within your power to protect this information?" To some extent, this nebulous definition can lead to legal debates of technical possibilities versus financial burden.

The Bottom Line

Though Massachusetts and Nevada are the first states to enact these strict data laws, the rest of the country is not too far behind. California—the largest state economy in the United States—has enacted a notification law as has Virginia, Iowa, and South Carolina among others. It would behoove businesses across the country who handle PII to prepare as if a nationwide requirement was on the horizon. It makes good business sense to not only secure customers' data to the fullest extent, but companies who are proactive in protecting their customers will retain their loyalty and their business.