KeepItSafe®

Helping Your Backup Process Address Regulatory Guidelines

Protecting your data is smart business, but it is also the law. Regulations now demand your organization have a backup procedure that includes frequent offsite backups, for example, and that your backed-up data must be tested regularly to ensure integrity and confidentiality. KeepItSafe® helps your backup processes address **federal regulations** and **guidelines** such as:

- HIPAA
- Graham Leach Bliley
- SEC Rule 17a-4
- Sarbanes-Oxley
- FINRA
- SAS 70

Here's how we do it:

- We store your data encrypted using 256 bit AES encryption at all times at highly secure offsite data center locations. The data is not subject to human error or tampering.
- The encryption code is not sent to our facilities, so even if they are hacked, no one will be able to access your data.
- All data is stored on high-end disk arrays and cannot be changed once it is backed up to our facilities.
- All backup and restore activity is captured in an audit trail.
- We restrict login privileges only to those with administrator credentials.
- Data integrity checks are done nightly to ensure that your data is being stored correctly.
- Retention rules can be setup based on a business's individual needs and can be configured down to the file level.

KeepItSafe offers comprehensive cloud data availability solutions — contact us

888 965 9988 | www.keepitsafe.com | sales@keepitsafe.com