5 Ways BasisCode Keeps Your Data Safe + Secure

With BasisCode as your compliance management system, you never have to worry about the security of your data.

We take numerous measures to maintain security against outside parties' unwanted attempts to access your data, as well as protect your privacy from those who do not have your consent to access your information.

https://basiscode.com/wp-content/uploads/2021/03/Tech-Talk.mp4

Here are 5 ways that BasisCode keeps your data safe and secure:

1. Encryption in Transit and at Rest

Encryption in transit protects your data if communications are intercepted while data moves between your site and our platform. This protection is achieved by encrypting the data before transmission, authenticating the endpoints, and decrypting and verifying the data on arrival.

Data is encrypted at rest as well as within our secure server environment via drive level encryption.

2. Disaster Recovery

In the event of a cyber-attack, natural disaster or business disruption, your data is one less thing you'll have to worry about. BasisCode's elaborate security planning enables us to protect your organization from the effects of significant negative events.

3. Real Time Replication

Real time replication is the instantaneous copying of data to one or more places as it is being generated. Because your data is replicated to a geographically alternate environment using SafeHaven technology, it would still be available to

you if your business were to experience a negative event.

4. SSO + MFA

With Single Sign On (SSO), our clients can decide to manage the authentication process to BasisCode via their own, internal security processes. Since security is managed on your end, no more forgotten passwords and pesky sign-in screens needed. Your internal systems verify your employees and securely hand them to BasisCode to manage their compliance needs.

As an alternative to SSO, Multi-Factor Authentication is used to add another level of security to the sign-in experience. Users can authenticate via a text message or phone call to their cell or by using app-based token providers such as Authenticator and Authy.

5. WORM

Write Once Read Many describes how BasisCode stores key data, in which information – once written – cannot be modified. This protection assures that your organization's data cannot be tampered with once it is written to the BasisCode platform.

BasisCode understands the necessity of various security methods to protect data from both inside and outside threats. We take pride in the safety of the data within the BasisCode platform, as well as bolstering the security of your company's most important information.

Schedule a demo today with BasisCode to significantly advance your compliance and risk management programs.