Security and Governance

Revver is great for storing, automating, and allowing you to securely collaborate on your documents. But the security of your data can't be overstated, and Revver comes with everything you need to protect your valuable documents and data. We use a shared responsibility model for security, meaning that Revver is designed to minimize the potential for security incidents, while providing our customers the tools they need to configure their security according to their requirements. In other words, Revver comes with standard security features, but also has configuration options for customers who need to adhere to a specific security standard.

Every Revver Customer is Provided with:

Encryption

Every file stored in Revver is encrypted, both in transit and resting. This ensures that only people with the appropriate access can see the contents of a file, regardless of where they access it.

Data Sovereignty

With different laws and regulations about where data can be stored, Revver has data hosting environments in several regions. These include the US, UK, Canada, and US Gov-Cloud for customers that require data to be stored and managed in the US only. Customers can choose the region that works best for them, so their data is right where they need it to be.

Maintenance

We're committed to maintaining Revver with the latest patches and updates so that your data is as secure as possible. Our Cloud environment ensures that these updates and patches are applied automatically.

Certifications

Our SOC 2 Type-II, ISO 27001, and FINRA certifications demonstrate that we've done the work to keep your data safe, so you can trust that our security will get the job done.

Features that Revver Customers can Configure:

Governance and Retention

Proper controls, permissions, and dispensation of sensitive client or employee data isn't just a nice feature to have, it's a requirement. Hanging on to files that should have been disposed of can be a serious security risk, if not a full on compliance issue. Revver can set automatic governance and retention policies as soon as the document is uploaded, so you don't have to worry about manually purging data.

Multi-Factor Authentication & Password Requirements

Based on government or industry requirements, you may need to set up requirements for passwords and leverage two-factor authentication. This can be configured within Revver and provides users with a safety net in case their password is weak or stolen.

Administrative Features

Beyond just password requirements, Revver has a suite of features that can be customized to fit your organization's security requirements. From whitelisting IP addresses, login times, setting the frequency of password changes, and more, you can rest easy knowing that Revver will automatically enforce your security requirements.

Access Controls

Sometimes granting access to a file or folder isn't enough. You may need to grant specific permissions, such as viewing rights while restricting editing rights. Revver's permission settings gives you total control over which users have access to which folders and files. **Role-based access controls** allow you to apply security policies based on user roles, so they automatically inherit access to the folders and documents they need and are restricted from accessing the files they don't.

Customer Compliance

Customers can leverage these features to configure their environments to be HIPAA, WORM, PCI, and GDPR compliant. We're happy to assist our customers as they set up their environments to achieve these levels of compliance.

Revver's security is designed to bring you peace of mind by helping you achieve your desired security outcomes. There's much more to our security that we're happy to talk with you about and how it can apply to your organization.

4101 North Thanksgiving Way
Suite 200
Lehi, UT 84043

www.RevverDocs.com