When you're using eFileCabinet, you can rest assured that your data is going to be safe and kept well-protected. To better understand how we secure and protect your data, here is a list of frequently asked security questions.

What level of encryption is used?

A: All data uploaded to Rubex is encrypted using **256-bit AES** while both resting and in-transit. We use an **SSL/TLS** connection to encrypt communications to ensure only the correct person can access that information.

What security options are available to admins?

A: Create security policies that can be applied system-wide or for specific users.
Password Requirements: Set requirements for password complexity and the frequency of password resets.
Two-Factor Authentication: Login with password and mobile authenticator application, or email token.
Specific IP Address: Create a whitelist of IP addresses that users can only access the system through.
Specific Login Times: Set specific days of the week and hours when users can access the system.
SSO Authentication: Require login to the system through compatible SSO service.

How does security affect compliance?

Rubex by eFileCabinet provides the tools to become **HIPAA**, **FINRA**, and **SOC 2 Type 1** compliant. Governance features are available so you can set retention dates and can automatically purge unnecessary data. Documents can also be locked down in **WORM** format so they cannot be deleted or tampered with.

How can I access a SOC 2 report?

SOC 2 reports are not public, and anyone who seeks to access this data must be prepared to sign a non-disclosure agreement. Contact an eFileCabinet representative to begin the process of obtaining a report.

Rubex by eFileCabinet is protecting your data 24/7 and is only accessible by those authorized to access it. We have created a customizable experience for you to access and store your data with the highest protection while helping you stay compliant and avoid liability.