FirmRoom

Security Specification Sheet

"FirmRoom was built to go beyond standard security measures. We understand the importance of keeping your data secure, accessible, and organized."

Data Protection

FirmRoom puts you in control. Manage users by controlling access to confidential documents.

Third-Party Examination Report	SOC 2®, Type 2 Report
Encryption of Data	256-bit encryption of all data both in transit and at rest
Secure Connections	All connections are protected using TLS with 256-bit symmetric encryption and 2048-bit authenticated key agreement
Password Protection	Passwords are masked and encrypted with Bcrypt
Data Center ProtectionOffsite Backup for Disaster Recovery	At data centers, all data remains encrypted using 256-bit AES, a certification used by the U.S. Government for top-secret documents
Offsite Backup for Disaster Recovery	All information is stored in multiple data centers which are located across locations in the United States and the European Union. This acts as a protection against hardware failure, theft, virus attacks, deletion, and natural disaster.
Privacy	FirmRoom never has back-end access to your data

aws Amazon Web Services

Amazon Web Services is the leader in cloud security. FirmRoom utilizes its security measures to provide you with the utmost protection possible, including third-party examination reports.

Secure Data Center Location	Locations in the United States and the European Union
Network Security	AWS has a diversified approach to network security: segmentation, firewalls, and intrusion detection, among others
Third-Party Examination Reports	Service Organization Control (SOC) reports 1, 2, & 3
ISO 27001 Certified Data Centers	Security measures onsite include: pin codes, keycards, biometric hand scans, and onsite security offices 24/7, 365

Additional Security Measures

We offer additional features to ensure you have the highest level of security.

Multi-Factor Authentication (MFA)	FirmRoom offers SMS authentication and authentication app options
SAML 2.0/Single-Sign-On (SSO)	Use Microsoft Active Directory, OneLogin, or Okata to access FirmRoom. Easily add or remove users from the system to enforce company-wide password policies.
Access Control	Restrict system access to ensure only certain users have access to specific information
Audit Logs	Track system activity by user, date, time, and action taken