File Portal Security

The SDFI File Portal is a secure, cloud-based solution for uploading, temporarily storing, and sharing encrypted forensic case files. Designed for forensic photography and evidence handling, it supports strict legal chain of custody requirements and aligns with regulatory compliance standards.

All SDFI Share Files are created through our Software Suite with security in mind. Users select requested evidence which is then packaged and encrypted with a user-generated One-Time Only Passphrase using AES-256-bit encryption. The package is then uploaded to the File Portal through encrypted channels, where they are temporarily stored in a secure cloud environment. Authorized Third Parties may download shared files via a secure link, but can only decrypt and view them after receiving the passphrase directly from the sender.

The SDFI File Portal utilizes the FilesAnywhere platform which provides a robust, enterprise-class cloud storage infrastructure, including:

- SOC-compliant data centers
- Multi-tiered network and intrusion protection
- Redundant storage and infrastructure systems
- Encryption of data in transit and at rest
- Administrative tools for secure user provisioning and audit logging

While FilesAnywhere supplies the core infrastructure and baseline security capabilities, SDFI enhances these protections by applying our own encryption standards and operational procedures before any data enters the system. As a result, neither SDFI nor FilesAnywhere have access to unencrypted forensic data, maintaining the legal and ethical boundaries required for forensic integrity.

The following pages contain the most recent FilesAnywhere security and compliance documentation to support and validate the infrastructure-level protections provided by our vendor.

SDFI-TeleMedicine LLC, 950 Pacific Ave, Suite 820, Tacoma, WA, 98402
Support@SDFI.com • 310-492-5372 • www.SDFI.com

FilesAnywhere

Industry Leading Security

Trust, Privacy, and Compliance Means Total Assurance

FilesAnywhere provides the necessary tools to **meet the most rigorous privacy,** security, and legal requirements allowing highly regulated industries, including **financial services, healthcare,** and government to work within a private **cloud environment.**

Is your data safe with FilesAnywhere? Absolutely. Since 1999, we've gone beyond standard measures to protect our customers and their data. Our unyielding commitment to security has made safe cloud storage possible. Thousands of businesses around the world use FilesAnywhere to store, access, and share data online. We deploy a blend of security measures to ensure maximum protection and the greatest overall data safety, including:

- Independent Security Evaluations
- Three-Tiered Code Validation
- Enterprise Class Data Center SOC 2 Certified
- TLS Encryption for all Secure Transfers
- 256 Data Encryption at Rest
- Multi-core Firewall Protection
- Network Intrusion Prevention System
- Automated Backup, Daily Snapshots, and Data Restore
- Role-Based Access Control
- 24/7/365 Data Center Monitoring

Centered Around Security

We've applied an extensive and meticulous level of security to protect our customers' files. Our datacenter is contained inside one of the best-connected hosting facilities in the world and is SOC 2 certified. This state-of-the-art, enterprise-class facility offers complete redundancy in power, HVAC, fire suppression, network connectivity, and security. Every item of hardware, system process, network port, virtual object, and every connection is monitored 24/7/365.

The average total cost per company that reported a breach last year was $4.0 million.

source: Ponemon Institute and Symantec

Thresholds and system capacities are also monitored with predictive alerts to our network operating center. N+1 redundancy prevents single point failure. Redundant backbone connections provide the highest performance connectivity.

Intrusion Detection and Prevention

Advanced, multi-tiered security protocols work together in layers to protect the network at all times. Security-monitoring software includes intrusion detection, virus scanning, system logs, and notifications of suspicious activities in real-time.

Compliance

Our approach is simple--make sure our practices exceed the expectations and requirements of the customers we serve. We have deployed security, encryption, and monitoring features within the application to help our clients meet compliance requirements, such as HIPAA , FINRA, GLBA, SOX, SSAE16, SKYHIGH, PCI, and IS027001.

In today's online environment, **customers** demand security. We take your privacy, and the safety of your data, very seriously. Vulnerabilities are tested daily by third-party security specialists.

FilesAnywhere

support@filesanywhere.com
Phone (888) 661-6565
www.filesanywhere.com

filesanywhere

Confidence in the Cloud

At FilesAnywhere, security is our #1 priority.

FilesAnywhere Security Protocols

Is your data safe with FilesAnywhere? Absolutely. Since 1999, we have gone beyond standard measures to protect our customers and their data. Our unyielding commitment has made safe cloud storage possible. Thousands of businesses and individuals around the world use FilesAnywhere to store, access, and share data online. We deploy a blend of security measures to ensure maximum protection and the greatest overall data safety.

- **Independent Security Evaluation** - SOC 3, ISO-27002, and HIPAA Compliant.
- **Three-Tiered Testing** - Rigorous QA processes to eliminate errors.
- **Data Encryption for Transfers** - 128/256-bit SSL is standard on every account.
- **Data Encryption at Rest** - Isilon proprietary storage cluster data encryption comes standard on business and enterprise accounts.
- **Firewall Protection** - IP authentication and brute force attack prevention.
- **Automated Backup** - Coolbackup encrypts data locally before uploading with AES 256-bit encryption
- **Daily Snapshots and Data Restore** - Taken each morning at 5:00 a.m. and stored for 30 days of point-in-time backup.
- **Role-Based Access Control** - Advanced user provisioning and permissions.
- **Data Center Monitoring** - State-of-the-art facility with 24/7/365 monitoring.

App & Network Security

In today's online environment, customers demand security. We take your privacy, and the safety of your data, very seriously. Grant folder and file access to users, groups, or guests. Create virtual folders that allow for hand-picked file access. Add an extra layer of security with optional link-based password protection, link expirations, and lifecycle rules for automatic deletion of folders and file. In addition, McAfee Virus scanning of all files and documents comes standard. In short, we employ best practices for total assurance.

Account Security

- Administrative auditing and reporting
- Access and usage metrics
- Automated email notifications
- Custom password lifecycle
- Custom password strength requirements
- User level provisioning and permission levels
- Division, department, and group segmentation

Network Security

- Server protection by industry standard firewall
- Access restricted to fixed IPs
- Regular external intrusion testing
- Redundant backbone connections for high performance connectivity
- Intrusion detection system monitored 24/7/365

Data Center Security

We've applied an extensive and meticulous level of security to ensure the safety of our customer's files. Our data center is contained inside one of the best-connected hosting facilities in the world and is SOC 3 compliant. This state-of-the-art, telco-class facility offers complete redundancy in power, HVAC, fire suppression, network connectivity, and security. Every item of hardware and every connection is monitored 24/7/365.

Redundancy and Fault Tolerance

- N+3 redundancy to prevent single point failure.
- Rack mount hard drive arrays running RAID 50 provide continuous hot-swap disk redundancy.
- Multiple layers of power redundancy prevent downtime from power loss to servers, storage, and networking equipment.

Version Integrity

- Enterprise accounts are protected by 125 separately saved versions.
- Standard 30 days of automated backups for all accounts.
- Users may opt to configure additional Version History protection.

Intrusion Detection and Prevention

- Advanced multi-tiered security protocols are working together in layers to protect the network at all times.
- Firewalls monitor each firebox firewall appliance.
- Security monitoring software running on server equipment includes intrusion detection, virus scanning, system logs, and provides notifications of suspicious activity in real-time.
- Protection from email attack, spam, and viruses.
- Daily vulnerability assessments track deviations from standard baseline, presently protecting our network from over 40,000 known vulnerabilities.

Highly Trained, Expert Teams

- Our information security team includes engineers trained in data security, encryption, risk prevention and incident response.
- Experts in security methodology, threat avoidance, detection, and response.

Compliance

Insufficient data management, ineffective workflow, transparency, and non-compliance are all problems that face companies today. Legacy systems require that the solution be molded to fit the problem. Private clouds are replacing traditional, on-premise systems from small businesses to large enterprises, and streamlining inefficiency. Even highly regulated industries, including financial services and healthcare, are able to migrate when data privacy, security implications, and legal and regulatory requirements are met.

Our approach to security standards is simple—to make sure our practices are even more thorough and more sophisticated than the customers we serve. Our data center is SOC 3 compliant meeting stringent criteria, and we have deployed security, encryption, and monitoring features within the application to help clients to meet the compliance requirements, including:

- HIPAA
- GLBA
- SOX
- SSA16
- PCI
- ISO27002

We employ the best practices to provide total assurance, delivering information privacy and standards compliance for our customers.

filesanywhere

sales@filesanywhere.com
Phone (855) 796-2669
www.filesanywhere.com