

# Confidence In the Cloud

At TranscriptionBox,  
security is our #1  
priority.

## TranscriptionBox Security Protocols

Is your data safe with TranscriptionBox? Absolutely. 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 TranscriptionBox 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.



[sales@transcriptionbox.com](mailto:sales@transcriptionbox.com)

Phone 877.611.6724

[www.transcriptionbox.com](http://www.transcriptionbox.com)