TitanFile Security Overview

TitanFile is committed to providing the most secure correspondence platform for our clients. We employ industry-recognized best practices, utilize NIST-approved encryption algorithms, and continuously innovate in the field of security to protect our client's confidential data.

1. ZERO KNOWLEDGE: CLIENT-SIDE ENCRYPTION

Client-side encryption (CSE) is a mechanism to encrypt files on the user's computer before they're sent to a service provider using encryption keys that are owned by the user. The service provider does not have access to these keys.

Unlike other cloud solutions where the vendor holds the keys to the encrypted files, TitanFile offers its clients zero-knowledge peace of mind. This means that TitanFile staff is unable to decrypt the client's files because only the client has access to the encryption keys. This removes the possibility of unintentional or unauthorized access to unencrypted data on the vendor side.

TitanFile's unique approach to in-browser encryption enables clients to use CSE without having to download or install any additional programs. A user's browser will encrypt files before they're sent through TitanFile. This is made possible by the new HTML5 Cryptography API standard.

2. NETWORK SECURITY: ENCRYPTION IN TRANSIT

On TitanFile login pages, your web browser establishes a secure transport-layer security (TLS) connection between your computer and our platform. When you leave a secure portion of our platform, you will get a notification from your Internet browser that you are leaving the secure section and returning to an open section.

All communication between client and server is performed over a 256-bit TLS connection. This is the strongest, most secure form of encryption that is generally available in Internet browsers on the market in North America today.

3. SYSTEM SECURITY: ENCRYPTION AT REST

All files uploaded and shared through TitanFile are encrypted before being stored on our servers. The file encryption uses algorithms and schemes that have been approved for encrypting and storing classified information up to the Top Secret level by all US government departments and agencies.

TitanFile encryption uses a combination of the AES encryption algorithm and the SHA-512 hashing algorithm. The AES algorithm that we use relies on a 256-bit encryption key, which provides for a much stronger protection than the 128-bit key typically used in commercial and consumer applications. The key itself is never stored on the same servers as the files. Therefore, if someone gains physical access to the servers and the storage disks, the data will be useless for them without the encryption key.

The Advanced Encryption Standard (AES) was published by National Institute of Standards and Technology (NIST) in a Federal Information Processing Standards Publication FIPS PUB 197 in 2001. SHA-512 is a secure hash standard that was designed by the National Security Agency (NSA) and published by NIST in FIPS PUB 180- 2 in 2002 and FIPS PUB 180-4 in 2012.

4. SECURITY AT THE FACILITIES: SELECTABLE DATA RESIDENCY

TitanFile clients can choose where they want their data stored. We currently offer data residency in Canada, United States, and on premise using the client's infrastructure.

4.1 CANADIAN DATA RESIDENCY:

TitanFile uses the Microsoft Azure infrastructure in Canada. The primary data center is in Toronto with a secondary data centre in Quebec City for backup, business continuity, and disaster recovery.

4.1.1 Data centre security:

- Monitored by external and internal CCTV cameras
- DVR system backed up by SAN storage
- Access control using access card and biometric authentication
- Mantrap in place for single person verification utilizing ultrasonic technology
- Intruder and door tampering alarms in place
- Secure managed loading dock
- 24x7x365 manned DCO onsite

4.1.2 Data centre certification:
SSAE 16, CSAE 3416, and ISAE 3402

4.2 UNITED STATES DATA RESIDENCY:
TitanFile relies on the secure Amazon Web Services (AWS) platform for hosting its service in the United States. AWS offers a high degree of compliance and certification. A full list can found at http://aws.amazon.com/compliance/.

5. EXTERNAL SECURITY AUDITS

TitanFile's platform undergoes regular external security audits. These audits include automated system security and configuration monitoring as well as penetration testing by certified independent security experts.

6. COMPLIANCE

HIPAA and HITECH compliance. TitanFile is fully compliant with the Health Information Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. For our clients who are Covered Entities under HIPAA, TitanFile offer Business Associate Agreements (BAA).

PIPEDA Compliance. TitanFile is fully compliant with the Canadian Personal Information Protection and Electronic Documents Act.

Curious how TitanFile can help YOUR business?
Get started by requesting a live demo from one of our experts.

TitanFile

+1-855-315-6012

sales@titanfile.com

www.titanfile.com

About TitanFile Inc.
TitanFile is an award-winning, easy and secure way for professionals to communicate without having to worry about security and privacy. TitanFile automatically organizes messages and documents around clients, groups or projects, reducing filing overhead and increasing productivity. Multi-level encryption, granular access control and full audit trails ensure compliance and make TitanFile the best choice for secure communications.