

completelyprivatefiles



As a privacy company, security and reliability is of critical importance to us. Our operations model, from hardware to software design, incorporates comprehensive steps to ensure that your data is secure, private, and can be accessed and encrypted or decrypted in a reliable manner. Our clients can have every confidence that their data is safe.

Questions?
Call 1-877-608-8988

Overview

completelyprivatefiles.com provides network-based encryption services to its clients. As a matter of necessity, security, privacy, and reliability have been built in at all levels of our service. We want our clients to be confident knowing that their data is protected, private, and accessible at every point that it is in contact with our system:

- Data center
- Network
- Application
- Privacy



Data center

completelyprivatefiles.com hosts its services at pair Networks, a world class hosting provider of long standing in Pittsburgh, Pennsylvania. They operate a dedicated, multi-homed, and fully switched datacenter, with five diverse backbone network providers.

Pair provides ongoing audits, 24x7x365 monitoring, daily backups, and network uptime in excess of 99.9%. Servers are hardened against security exploits, and reside behind firewalls. Physical access to servers is restricted and site monitoring takes place around the clock.

The datacenter features redundant climate control, automatic fire suppression system, continuous, clean power via UPS, and redundant failover generators.

Network

Access to our encryption services takes place using **256-bit Secure Socket Layer (SSL)** encryption at the network level. This ensures that all data transferred between our systems and our clients are fully secured with unbreakable, industry standard encryption.

Application

User authentication: completelyprivatefiles.com incorporates “best practice” strong user authentication for access to its systems. End users are required to create a username and password pair, while service providers and developers are assigned a 256-bit API token.

In-memory encryption: Encryption or decryption occurs while the data is in memory. No data is ever actually stored on disk, except in specific cases. In the case of the API, the only time data is stored to disk is at the request of the service provider, and then only encrypted data is stored on disk.

API access: Our API uses a session-based design that allows developers and service providers to first authenticate, and then allow their users to interact with our services through a session token. This gives providers the flexibility they need while providing a secure API model.

Key logging: When a piece of data is encrypted or decrypted, the key is logged into our database system using a transactional process to allow for rollback. At the same time, the key also is logged in a *geographically remote location* via secure transmission over the Internet. At no point should a key ever be lost.

Privacy

Customer privacy is paramount to completelyprivatefiles.com. We have developed a comprehensive privacy policy to protect our customers and explain our view towards personal information. **Our current privacy policy is viewable at www.completelyprivatefiles.com.**