Re: Data Security Representation by LeapFILE, Inc.,

This letter is a summary of security measures taken by LeapFILE to guard the privacy and integrity of customer data that is managed in the regular course of business.

Overview

LeapFILE implements several layers of security to ensure confidentiality during the file transfer process. Each layer of protection reinforces other layers to create a comprehensive security net that protects data, authenticates users, enforces granular access to information, and automatically produces a detailed audit trail of changes in file custody.

Protection Layer

The first layer of security protects data in custody from unauthorized access. This provides the foundation for controlling access to information by blocking all access points. The service implements the following security measures for protection:

Physical Access Control

Physical access to systems containing confidential files is controlled and monitored. The service is housed in state-of-the-art data centers featuring 24x7 guarded access facilities using a wide range of security systems including video camera surveillance and the latest in iris and palm scanning technologies. Further discussion on our data center, Rackspace, is made below.

Network Access Control

Network access to systems is highly restricted. The service utilizes firewalls to shield servers from the Internet and restricting access to only HTTP ports. This denies any network-based access to systems that may compromise security.

Data Storage

Files are stored in an encrypted format for added protection. The service uses AES, a federal government standard for private-key or symmetric cryptography. Even if someone gained unauthorized access to a file, the information contained in the files will remain confidential.

Data Transmission

Data transmissions over any network are always encrypted. Files are uploaded and downloaded from the service using SSL encryption.

Data Retention

To limit exposure, the system enforces a strict data retention policy. Each file transfer contains an expiration date ranging from 1 to 14 days based on user preference. If a file is not downloaded before the expiration date, the file is automatically and permanently deleted. If a file is successfully downloaded, the file is automatically and permanently

deleted after 8 hours. For more control, users can cancel a file transfer and delete the associated files at any time.

Authentication Layer

The next layer of security beyond protection is authentication. This consists of security measures to validate user identity before granting access to protected information. There are two types of users that require authentication: internal users that have LeapFILE accounts and external users that exchange files with internal users.

Internal User Authentication

Each internal user is assigned a unique ID and password for authentication. Passwords are required to be least 6 characters to ensure integrity. Stronger passwords can be set at the user's discretion. In addition, passwords are encrypted to ensure integrity.

External User/Receiver Authentication

Instead of traditional ID and password authentication, each file transfer carries its own authentication requirements (link, tracking code, email, access code), which compartmentalizes access and simplifies authentication. To download a file, the receiver must first have the secure download link or the tracking code. This is the first form of ID. To prevent unauthorized users from guessing the ID or secure download link, the receiver must also provide the matching receiver's email address. This is the second form of ID. At minimum, a receiver must provide at least these two forms of ID to access any download. For even more protection, the sender can also set an access code for each file transfer. This is the third form of ID. The access code can be unique to each transfer or utilize confidential information like an account number known by both the sender and receiver. The access code is also encrypted to ensure integrity.

Authorization Layer

The authorization layer works in conjunction with authentication and protection to enforce granular access to information. Each user must authenticate to start a session every time they use the service. The session carries user credentials that are compared against permissions for every request. This enables the service to enforce permissions at the application level for restricting access to authenticated users only.

Audit Layer

The audit layer automatically records the time, IP address, and user name for every file download. This is compiled for every file transfer and made available to the user for tracking file custody. The service also automatically sends an email alert to the sender when the file is successfully downloaded.

SAS70 Type II Certified Data Center

Rackspace is a leading provider of web applications and software as a service for on-demand companies, like LeapFILE. Specifically, LeapFILE has qualified for and is a customer of Rackspace's Intensive Hosting Services.

They support thousands of applications, millions of users, and billions of transactions on a daily basis. Rackspace has invested millions of dollars in complex and expensive infrastructure necessary to deliver applications over the Web. Rackspace has obtained SAS70 Type II Certification.

Access LeapFILE Servers, Information and System Resources

LeapFILE's servers reside in the U.S. locations of Rackspace, and specifically in San Antonio, Texas. Rackspace has employed internal controls that limit, control, monitor and document access to Rackspace employees. See SAS70 Report.

Pursuant to Rackspace's internal controls, LeapFILE is not permitted any physical access to its servers or the data center except under very specific procedural guidelines. For all intent and purposes, LeapFILE accesses its servers remotely. Such network access is currently limited to LeapFILE's CEO and limited to necessary and ongoing support of LeapFILE's applications and services. A record of all network access by LeapFILE is maintained and available to LeapFILE customers upon request.

I hope and trust that this satisfies your compliance review.

LeapFILE, Inc.
www.leapfile.com
support@leapfile.com
1-888-716-9380