AGILELAW
Practice litigation, not litigation support

Comprehensive Security Program

Our application was designed to ensure maximum security for every document uploaded to our servers. With our comprehensive approach to security, data will never end up in the wrong hands.

1. Data Transmission

All data transmitted between the user and our servers, and between servers, is encrypted via industry standard 256-bit SSL/TLS 1.1 encryption. This includes all interprocess communication between servers.

2. Data Isolation

Each customer's data is stored in the database with its own unique key. No data is accessible, even to our own servers, without this key. This key is only granted during an active user session and is revoked upon logout. A separate, isolated server process – that itself has no customer data access rights – is responsible for granting access to this key at the time of user authentication. In addition, encrypted documents are stored in a separate database for each customer, adding another layer of isolation. Storing all customer data with this separation prevents malicious or inadvertent unauthorized exposure of any and all data.

3. Document Storage

AgileLaw uses 256-bit AES encryption (specifically, rijndael-128 with 128-bit block size and a 256-bit key) to encrypt every document with a unique, randomly-generated 32 byte key. The key to decrypt each document is never stored in plaintext on our servers. Instead, an encrypted version of the key for each document is itself encrypted with the user's password (which is stored as a one-way hash and cannot be decrypted). This means only an authenticated, logged-in user has the key required to decrypt her documents. Other users outside of the firm, and even AgileLaw system administrators, do not have the ability to decrypt other tenant's documents. In addition, having keys for each individual document allows for selective sharing of chosen documents during a deposition while keeping the remainder private.

4. Local Storage

AgileLaw does not store or cache any documents on users' local computers or tablets. Once a user is logged out, previously-viewed documents can no longer be viewed on the device.

5. Network Security

AgileLaw utilizes Rackspace's Cloud Networks to create an isolated, multi-tiered, virtual Layer 2 network (powered by OpenStack, leveraging Open vSwitch, and managed by Nicira's Network Virtualization Platform) for our production environment. Our web application and database servers are therefore on an isolated network that filters out illegitimate traffic.

6. Password Security

AgileLaw enforces the following industry-standard password complexity to control system access:

- Minimum length of 8 characters
- At least one capital letter
- At least one lowercase letter
- At least one non-alpha character

Additionally, user passwords are never stored in plaintext in our system. Instead, password hashes are stored using the blowfish asymmetric cipher with a high number of iterations to increase the cost and decrease the potential success of brute-force attacks. Each password is individually salted with 32 random bytes to hinder modern rainbow-table based attacks. What this means is that without the user's unique email and password combination, the outer level keys can never be decrypted. Without knowledge of the original, complex password, the document data is unreadable.

7. Password Recovery

AgileLaw recommends, but does not require, that each user chooses a series of 3 security questions with answers to those questions. Answering these questions provides the user with an ability to reset her password should she forget it. The combination of the 3 questions and answers essentially become a second "password" that can be used to reset a forgotten password. Should the user choose not to answer these questions, or if she forgets the answers to them, the only way to regain access is for an administrative user of the same firm to reset her password. In the event that all users for a particular firm forget their passwords and answers to the security questions, all documents associated to that firm's account are unrecoverable.