



Security Document

August 16, 2010



State-of-the-art Security for Legal Data

At GettingLegalDone, we understand the need for security in legal information systems: security from unauthorized access by third-parties, security within teams, and security from accidental data loss. We constantly review and assess our software and hardware in order to maintain a system that can respond to any threat level.

No system can guarantee perfect protection; maintaining security is always a joint venture between the company that provides a system and those who use it. The most common security breach occurs because of easily guessed passwords or passwords that are written down and left in plain view on the user's desk. A recent study showed that the most common password among Internet users is *123456*. The second most common? *12345*. The names of children and pets are also so common as passwords that in some cases an intruder can obtain access to a system in fewer than half-a-dozen guesses. Users must do their part in order to keep their data safe.

The Question of On-line Data Storage

Many people believe that it is inherently more risky to use an on-line system than to keep all data on a local hard drive or on a network server. However, we believe that on-line storage is actually *more* secure than local storage for the following reasons:

- Local data is often copied to laptops, smartphones, USB drives and other portable media that are easily lost or stolen. With on-line storage, the data is accessible to authorized users from any computer with Internet access, so there is rarely a need to make local copies that can fall into the wrong hands.
- Local data can be trapped in personal "silos" and lost unexpectedly. For example, if sensitive documents or spreadsheets are stored on a user's local hard drive, the odds are high that if the local drive crashes, the data will be lost. A study by Carnegie Mellon indicates that hard drive failure rates may be as high as 13%; only 26% of corporate IT departments report that local hard drives are regularly backed up.
- Another scenario involves the use of Outlook to track critical information such as review dates for contract review. The dates are kept in a particular user's Outlook account; when that user leaves the company, his now-closed account is not accessible to coworkers, and in many cases the information is essentially lost. Managing such dates and other information in a shared, on-line system protects against such surprises.

Secure Communications

When trusting your data to an on-line system, it is important that your information not be transmitted as "cleartext"; i.e., plain text that can be read by anyone who manages to intercept the data en route. The GettingLegalDone website (the "Site") is secured with 256-bit encryption using Secure Sockets Layer (SSL), the most widely used Internet standard for securing sensitive web data communications.



Access Restrictions

Access to the Site is restricted to users who have registered and supplied a valid and verified email address. Furthermore, public email accounts such as Gmail and Yahoo mail are not accepted for registration purposes, reducing the chances that a user with malign intent will be able to register without providing a traceable email address. Finally, only members of the Association of Corporate Counsel (and their authorized team members) are eligible for registration.

Domain Administration

Each user domain has a single domain administrator (by default, the first user from the domain to register at the Site). Subsequent users from such domain may only complete the registration process after approval by the domain administrator. All users at a common domain are referred to collectively as a "Team" and individually as "Team Members". The domain administrator may "lock out" any Team Member at any time (for example, in the event of termination). ***To protect Team data, it is imperative that lockout be made part of the organization's termination procedures.***

Data Segregation

User data is accessible only by the user who created such data and other users who are members of that user's Team. Furthermore, a user may classify certain data as "private," meaning that only that user (and not other Team Members) may view the data. A user's identity is determined on the server by session-based identification. Sessions are automatically expired after a fixed period of inactivity.

Direct user access to the database is never permitted.

Secure Document Delete

The reliable deletion of data can be as important as its preservation. In particular, when complying with a discovery request, you need to be sure that copies of old documents and emails are not lingering on a third-party server where they can be recovered by forensic data experts. When you delete a document, we overwrite the file 22 times with random byte patterns before deleting it at the file-system level. The United States Department of Defense requires only a seven-pass overwrite.

Third-Party Access Prevention

We utilize state-of-the-art firewalls, network monitoring, and intrusion detection tools. Strict change management rules are used and internal security policies and procedures are enforced.

Hosting Infrastructure and Physical Security

The hosting infrastructure used for GettingLegalDone is co-located at the Houston installations of Data Foundry, Inc. The set up offers the following:

Backbone Links

45 mbps – Time Warner OC3 – MCI and Sprint transit
45 mbps – UUNet DS3 (Houston)



45 mbps – Level 3
45 mbps – Insync Houston – Austin DS3
45 mbps – Insync Houston – Dallas DS3
45 mbps – Exodus DS3 exit point

Redundancy

BGP4 for optimal route selection and resiliency
Redundant border routers (Cisco 7507)
Redundant core routing switches using HSRP (Cisco 6509)
Redundant co-location switches for diverse Layer 2 links (Cisco 6509)

Redundant Web servers
Redundant Database server
Redundant DNS servers
Redundant mail services

Data Backup

Hard Drive Raid10 for Database/Application server
Overnight/Daily replication of web sites and databases
Overnight backup of critical data to optical storage

Power Backup

UPS

Exide Electronics Model 2045 uninterruptible power supply
80 k Va @ 480 volts load capacity
2 HR POWER CAPACITY AT 60 % LOAD

No. of Generators
Fuel Capacity

Two 1,000 kW Detroit Diesels
5,000 gallons

Physical Security

Co-location Area access

Co-location area is secured via a biometric access control system. Access to the co-location area and the floor is provided 24/7

Building Access

Security personnel on staff 24/7. After hours access to the building is logged and card controlled.

Data Security

Cisco fire wall

SSL (Secure Socket Layer) for encrypted web conten