APPLICATION SERVICE PROVIDERS
FOR ONLINE DATA STORAGE

An Application Service Provider (ASP) is an Internet-based electronic service that backs up your entire system automatically and stores the data on the Internet in a secure form and location. This online data storage method for backup and recovery has generated much discussion in legal circles. Online data storage can provide access to documents in a way that offsite backup cannot – especially if your offsite backup is stored in your same town or locale. This is one of the many tragic lessons learned in the wake of Hurricane Katrina, when one-third of the lawyers in Louisiana lost their offices, libraries, computers, client files, and homes. Even if the lawyers had backup devices or CDs at their home or other local site, few were able to access the backups. The ability of displaced lawyers to retrieve their client documents and financial data through the use of ASPs provides a powerful incentive to consider this alternative.

Online backup for PCs and servers can provide up-to-the-minute data backup protection; however, many lawyers have reservations about using ASPs. Generally, the security issues associated with storage are the main concern. Placing client information in the hands of third parties, the solvency of the provider, the security of the storage location, the method of storage, and the preservation of confidentiality are high on the list of reasonable concerns considered by lawyers. These concerns apply whether lawyers are storing paper files in a document storage facility or storing electronic data through an ASP. With a paper document storage facility, once you are confident that the facility either has no access to your stored documents or maintains confidentiality and privacy, you turn over the boxes of client files for storage and periodic retrieval. Placing electronic client data in the hands of third parties who remotely upload it to their Web site is really not any different. Proper security is crucial for each. A hacker can access an electronic site that isn’t secure; a thief can break into and enter a paper storage facility that isn’t secure.

Both a physical storage center and an ASP provide the user with a special key. An ASP’s security can be so restrictive that the user may be the only person who has the “key” – an aspect of storage that requires thought, planning, and safeguarding. There may be no electronic “locksmith” to help you enter your “storage facility” if the key is lost. Therefore, if you are the only key holder, you should store the key (usually a password) locally somewhere that is secure, such as a safe deposit box, and also somewhere secure in another geographic area. Don’t rely on your memory – this is a key (password) you hopefully will never have to use.

When choosing an automated, online data backup, storage, and restore system, ask these questions:

- Does the system offer the highest form of security data encryption available in the United States: Advanced Encryption Standard (AES)?
- Does the system offer a private encryption key that is held only by your office?
- Does the system encrypt all transmitted data at the source?
- Does the system provide continuous, automatic backups?
- Does the system have the capability to back up time-sensitive data like open files, e-mails, and databases?
- Does the system provide full coverage for complete data protection and recovery, including backup, offsite storage, ability to restore data over the network or dedicated storage device, online remote recovery, and offline archiving and recovery?
- Does the system provide instant file restores 24 hours a day, 7 days a week, 365 days a year?
- Does the system provide automatic notification of exceptions or problems encountered?
- Does the system provide detailed activity reports?
- Is the ASP’s server in a geographic location that is separate from your locale?
- Does the ASP take precautions for disasters in its own area, such as backing up on a server in another location?
- Is the ASP’s physical site secure? (The highest level of security is a Tier One Data Center Facility.)
- Is there a secure way for your firm to access the stored information if someone loses the law firm encryption key?