

Security FAQ

NetDocuments provides the highest Service Level Agreement for document security, privacy, integrity and high availability to your documents, e-mails and digital records than any service currently available for law firms.

Q: Who owns the documents when hosted in your data centers?

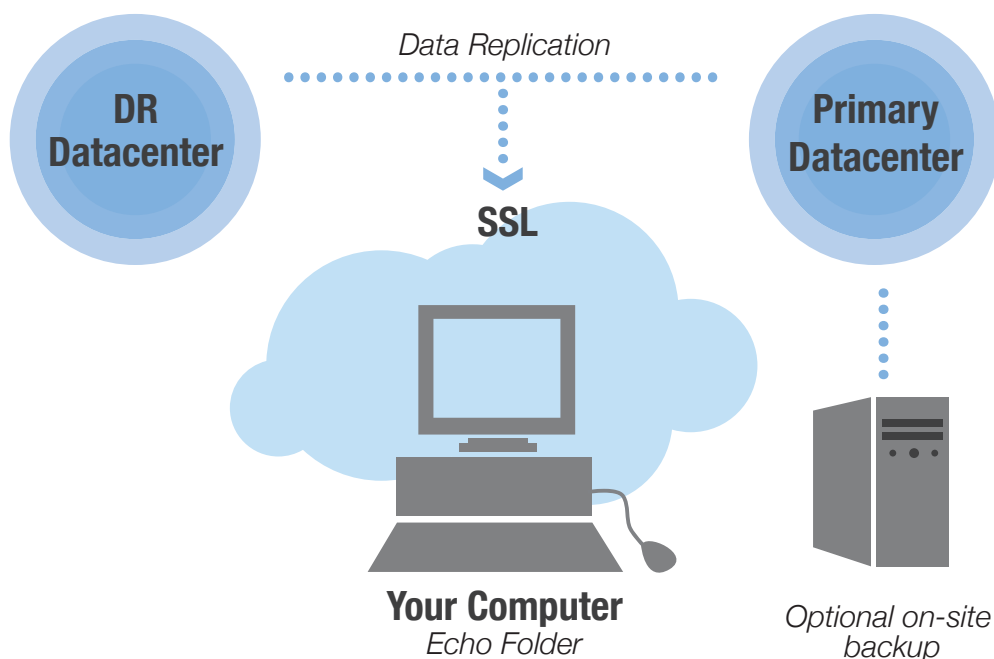
A: Your firm owns the documents. We are simply custodians of your documents. Only the firm has access to your documents.

Q: Who will manage my data?

A: You will continue to manage and administer your own data. The creation of users, user groups, document profile data, mass changes, cabinet and workspace creation, policies for security and record retention, and all other administration tasks will be controlled by your staff. The NetDocuments service relieves you from managing and maintaining servers, updating operating systems, updating application software, capacity planning, security enforcement, and other trivial tasks.



NetDocuments Cloud Architecture



Q: Does NetDocuments have internal policies ensuring information privacy and confidentiality?

A: The information you store in NetDocuments, referred to in the NetDocuments Service Level Agreement as Customer Digital Files (CDF), are owned by your firm, the organization as identified in the NetDocuments repository administration screens. NetDocuments and the data center operations employees do not view, disclose, divulge, release, e-mail, copy, duplicate, reproduce, send or transfer a CDF in whole or in part to any third party without the express permission of the data owner.

On rare occasions data owners will request and authorize NetDocuments personnel to access CDF content for support, validation, data upload, debugging and other reasons. Each workstation is capable of echoing any and all documents opened in the last few months (time length determined by the firm administrator), making the documents available for business continuity.

“The bottom line is, your documents will be much more available via NetDocuments than through your existing DMS.”

While it is understood that for support purposes certain CDFs may be accessible by NetDocuments employees, it is a NetDocuments policy that employees are forbidden to view, read, discuss or expose the document contents, unless the nature of the support requirement is such that reading the contents is absolutely mandatory. In such situation, the employee must have prior written permission to read the CDF contents from the information owner via a formal access grant in the NetDocuments service and from an express authorization by a NetDocuments Officer.

NetDocuments has achieved SAS 70 Type II and Truste EU Safe Harbor Certifications, acknowledging that NetDocuments delivers its SaaS content management service and its web site in accordance with these standards and rigorous audits. SAS 70 has evolved to a new standard named SSAE 16.

Q: Does the NetDocuments service ever go down?

A: NetDocuments has experienced 99.995% service availability, excluding scheduled down times, during the past many years. There are two world-class data centers for NetDocuments, one managed by LexisNexis, and one in the West managed by a federally-regulated commercial bank. These centers are managed 365x24x7 by a combined staff of 700 IT experts, and equipped with fully redundant ISPs, networks, servers, storage power & cooling, and security infrastructure. Data is replicated automatically between the two data centers, with the ability of each facility to service 100% of the processing loads.

In addition to recommending that firms acquire two independent Internet connections for high availability to greatly reduce the eventuality of Internet down time, users can continue editing existing documents or create new documents off line through the NetDocuments Echoing technology.

Q: Can I ever lose documents?

A: No, you will never lose documents. Unlike other document systems, while editing documents, the NetDocuments service will always automatically save a document locally into your Workstation disk first, then upload it the global data center, and finally obtain confirmation that the information has positively and definitively arrived in the repository before closing the transaction. Once in the data center, NetDocuments has a sophisticated world-class mechanism to maintain the integrity of the document via non-repudiation technologies.

NetDocuments has also developed the “Check-in List” technology, ensuring that multiple documents edited in the workstation simultaneously will always be accounted for, even during power failures or Internet-service interruption. If the Internet is down, users can continue creating new documents or edit existing ones, and the service will automatically auto-synchronize them into the repository when the Internet is restored and when the user logs back into NetDocuments.

NetDocuments also provides “concurrency control,” avoiding a second user from inadvertently changing the contents of a document while it is being edited by someone else, and ensures upload integrity via “check-sum” technology.



*World Class
Data Centers*





Q: Can you prevent NetDocuments or LexisNexis IT staff from reading my documents?

A: Absolutely yes. NetDocuments or LexisNexis IT personnel cannot read your documents. Employees are segregated into multiple classes, each with his own access privileges. Those with physical access to the data centers will not have operating access to the servers, and vice versa. Operators with access to certain service components do not have access to other critical service modules, ensuring no single person, without collusion with other individuals from potentially separate companies, will be able to locate documents.

Documents are encrypted in storage to make them non-legible. And the file's locations are obfuscated by being randomized against a 1.6 million directory structure on disk, making it practically impossible for someone to locate a specific target file. And an "audit trail" of all operator actions are recorded as well.

Additionally, If a customer deploys an Archived Cabinet, NetDocuments secures the cabinet as a virtual WORM storage container, where electronic files can be written once, read many times, but never altered or deleted, prohibiting even the customer's systems administrators to remove or modify such files. Policy-based retention rules would be the only method of purging records.

Q: Can someone unauthorized read my documents?

A: No, NetDocuments does not allow unauthorized access to any document. The repository supports strong authentication policies and specific access control for individuals and/or groups at the document or container level (access control can be set for a folder, workspace, client & matter, practice group, office, author or cabinet levels, etc). Ethical walls can be set up automatically excluding access to individuals or groups for any document, client & matter or any other profile metadata.

Q: Can you ensure that no one will read my documents while they are being transferred via the internet?

A: All documents are fully encrypted while in transit using secure SSL (secured socket layer). No communications between the Global Data Centers and the workstation will ever be clear-text.

Q: What if I inadvertently change a document; can I recover it?

A: NetDocuments maintains 30 instances of a document on-line, one for every day of the last month. These are called "snapshots," and they are independent of the document versions. At any time a user may recover from his or her own inadvertent edits.

Q: If your index becomes corrupted, is there the possibility of you serving up a document to an unauthorized user?

A: NetDocuments has never, nor will ever, deliver a document to an unauthorized user, even in the remote eventuality of a massive database and index corruption. A NetDocuments technology patent makes this an impossible scenario by physically "binding" a document and its access control into the same file. Even if massive corruption at the database or index were possible, the physical files still maintain the access control and ethical walls associated with that document.

Frequently asked questions ?

THIS WAY ~or~

THAT WAY

Bank-Level Security

NetDocuments technology will always perform a last and final check when “unobfuscating” the document to verify the permission of the user. Even if the service mandates a delivery to a particular user, if the internal permission list bound into the file does not match the mandate, the service will block the unauthorized delivery.

Q: Can anyone hack into your system?

A: No one has ever hacked into NetDocuments. Every precaution has been put in place, including dual firewalls, intrusion prevention, regular vulnerability and penetration tests, server security hardening, Ernst & Young certifications, and audits by bank regulatory agencies such as the Office of the Currency and Comptroller, Federal Reserve System, etc. In order for someone to hack into the system they would need to do the following: (1) break into the atrium firewall, (2) bypass the intrusion prevention system, (3) penetrate the Unix encryption hardware, (4) break into the Windows® 2003 and Microsoft® IIS security, (5) break into the DMZ firewall, (6) compromise the NetWare system, (7) decrypt the NDS secret store, (8) hack into the storage server security, (9) correctly guess a randomized number between 1 and 1.6 million, and (10) do this fast enough to avoid detection by the security monitoring personnel. If successful, the hacker will be disappointed because the file is obfuscated.

Q: What if I inadvertently change a document; can I recover it?

A: NetDocuments maintains 30 instances of a document on-line, one for every day of the last month. These are called “snapshots,” and they are independent of the document versions. At any time a user may recover from his or her own inadvertent edits.



Q: Can I have my documents stored locally inside my firm?

A: You can optionally install the NetDocuments Local Document Service, which will store all your documents locally at your premises. This will give you the peace of mind of knowing you have physical possession of all your documents at a site of your choice. For added peace of mind, your documents are also stored in extremely secure world-class data centers, the LexisNexis facility and in a federally regulated, commercial bank data center, for business continuity purposes.

Q: How easy will it be to get my documents out of your system if we choose to go another direction?

A: In the Local Document Service you will have every one of your documents in native mode, on your premises, organized into windows folders such as office, author, client and matter. There is also an XML file associated with each document, containing the profile metadata and access control list.

Q: Does the SaaS model compromise the attorney-client privilege?

A: The following was published Feb 9, 2006, by the Nevada State Bar: “On Remote Servers Under Third-Party Control: A law firm may store its electronic client records on a remote server under the control of a third party so long as the firm selects with care a company that promises to keep the information confidential.”

Q: Does the SaaS model compromise the attorney-client confidentiality?

A: The ABA Format Ethics Opinion 95-398 states: “The lawyer’s duty of confidentiality is not breached by giving a computer maintenance company access to a lawyer’s confidential records, so long as the lawyer is reasonable and competent in creating and maintaining the arrangement with the outside contractor.”