The Service Standards of Excellence for Content Management Cloud Computing

June 2011

The Service Standards of Excellence

In today's economic environment, the prime directive for organizations is to do *more with less*--more functionality, more computing power, better security, higher availability and business continuity, better global accessibility, and more storage capacity. The need to have more predictability with the overall IT costs is a must as well. And at the same time there are demands about cutting IT expenses as it relates to the demands of less maintenance, less hardware and software purchases, reducing the overall total costs of ownership, consulting services and capital investments. In summary, it's providing *more with less*.

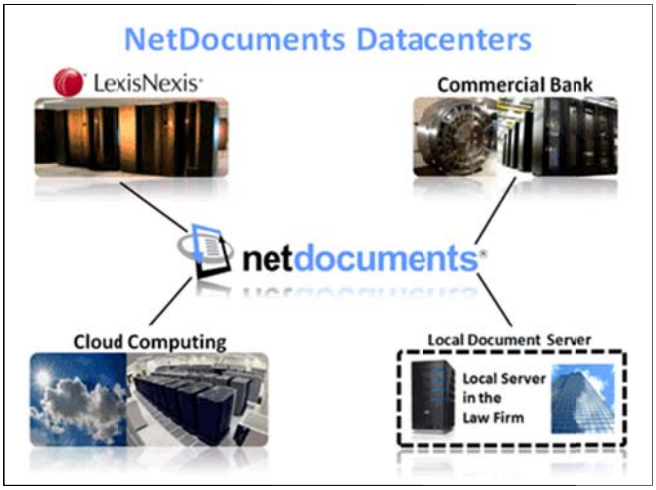
Software-as-a-Service (SaaS) and Cloud Computing is the answer. Leading Web applications such as NetDocuments, along with Salesforce, Google, etc., run on a single code base and infrastructure shared by all users. This type of environment allows for high scalability and faster innovation at a lower cost. With the growth of cloud computing the responsibility of the vendor is ever so important to ensure that it has met the highest standards of service related to business continuity and availability, trust and transparency, world-class security, document integrity and privacy, compliance, scalability, and performance.

NetDocuments is a leader in enterprise content and document management. With over 13 years' experience, the company is well trained and has met the test of time in every aspect of service delivery. After all, that is the heart and core of NetDocuments. NetDocuments was founded and designed from the ground up to service customers.

Business Continuity and Availability

There may be no better reason to migrate to the Cloud and SaaS applications than simply to ensure your documents are protected and secured from disaster. Being seen to be a resilient organization represents a competitive advantage in dealing with clients and that alone should increase any expected return.

- The NetDocuments primary global datacenter facility is a world-class facility hosting all documents, emails, and images accessible via the Web. Any equipment, network, or operating system failures will trigger a local backup system to take over operations.
- The NetDocuments secondary D/R global datacenter is also a world-class datacenter capable of supporting 100% of all NetDocuments users. Documents are stored simultaneously in both datacenters through continuous data replication via high speed VPN. The D/R facility is always ready to take full operational control in case the primary facility is incapacitated.



- Additionally a customer may deploy the NetDocuments Local Document Service, optional software physically installed in a local server at the customer's premise mirroring the contents of the global datacenters. *Refer to the NetDocuments Local Document Service datasheet for more detail.*
- Lastly, at the local workstation PC, each user has "echoing" enabled where all documents accessed by the user within a defined recent period of time (configurable by the administrator) are automatically stored for redundancy and performance.

The elapsed time from disaster to document availability will be immediate and instantaneous (i.e., zero seconds). The NetDocuments user interface is the same under normal conditions or in a disaster, eliminating any retraining issues. The equipment required in a disaster situation is any workstation (home or other location) or Internet device (BlackBerry or PDA), accessible anywhere, with full access to the document repository.

Primary Hosted Global Datacenter – LexisNexis

The primary NetDocuments datacenter is hosted by LexisNexis, a Reid Elsevier company, housing the most comprehensive collections of online information in the world, generating over $1billion in revenues, and storing over 5 billion documents of source information. The complex includes 22 MVS IBM operating systems, 300 mid-range UNIX servers, and over 1000 multi-processor Windows servers, serving more than 800 million customer searches annually. The primary datacenter hub consists of 45,000 square feet of raised floor, plus 22,000 square feet of electrical/mechanical equipment, backup by a secondary datacenter located nearby with 60,000 square feet of raised floor. The datacenter hardware, software and electrical/mechanical systems are engineered with multiple levels of redundancy to provide uninterrupted service in the event a single component fails. The systems are tested and maintained routinely to ensure they perform properly in case of an emergency. In addition, all critical data is copied and stored off-site and emergency business-resumption plans are tested multiple times per year.

There is over 650 full-time staff providing datacenter and telecommunications management and control of the entire complex. System management services are provided 365 days a year, 24 hours a day by a staff of skilled operations engineers.

Additional specialists are available, on site or on call, to provide the very best system support. The datacenter offers world-class fire detection and suppression systems with zoned smoke detection and Halon fire suppressions above and below the raised floor and a dry pipe sprinkler system. The building is rated to withstand up to 200 mph wind. LexisNexis facilities staff members focus on continuous improvement, so that customer experience is always positive. LexisNexis invests heavily in protection architecture to prevent worms, viruses, and hacking attempts. Additional security studies are conducted by third party contractors. LexisNexis datacenter today services 99% of the AM Law 100 firms.

Secondary D/R Hosted Global Datacenter – U.S. Commercial National Bank

Located in the intermountain region, the disaster recovery datacenter is hosted by a U.S. commercial national bank. A critical decision made early on during the architectural phases of NetDocuments was the physical co-location of a datacenter servicing secured, private documents in a federally-regulated commercial bank hosting facility. In fact, NetDocuments servers are literally placed in the highly secured room where all the financial operations of the commercial bank area are performed.

The rules and regulations imposed by the federal regulatory agencies on bank data are also imposed on NetDocuments data, which in turn also benefits the primary datacenter. There is an additional advantage of being co-located in the secured room at a bank. A critical issue is the presence of enforced policies and procedures, approved by the Courts, for dealing with currency and contents of safe deposit boxes. Documents stored in NetDocuments are simply considered assets stored in the bank's online safe deposit box.

Unlike other commercial DP hosting facilities, banks are completely prepared to deal with subpoenas, escheatment, and death of the owner, divorce proceedings, loss of digital certificates, and other legal actions. With a staff of 200 full-time employees, the bank's IT staff provides the datacenter with the networking, operations, and telecommunications management and control for the complex. Its Local Network Operations Center provides 365x24x7 onsite presence and management. A dedicated staff of 15 technology security experts secures the data from any and all unauthorized access. This team reports directly to the bank's president, instead of the bank's CIO for regulatory compliance reasons.

Data Replication between Primary and D/R Hosting Sites

All documents, emails, images, records, database, and index data stored in any of the global datacenters are automatically replicated to the other via a high-bandwidth dedicated secured VPN. This architecture ensures that all customer data is stored in two world-class datacenters without any single point of failure. NetDocuments customers

may have the peace of mind knowing that each of the redundant datacenters is capable of supporting the entire processing load for all users at any time.

24x7 Operations

Except for routine maintenance performed in the middle of the night and weekend evenings, the global datacenter will operate non-stop 24x7 for the entire year. Routine maintenance is planned well in advance, and users may still continue using the Echo folder on the workstation where the most recently opened documents are copied. Routine maintenance usually happens four times a year. NetDocuments continuously monitors the global datacenter to ensure its reliability and availability. NetDocuments deploys "robots" or software agents running in computers located in different parts of the world, which logs into the service every five minutes, and performs a series of multi-step operations exercising all major components of the service. Such robots will automatically alert a series of individuals at different levels reporting any slowdown of performance or its inability to perform certain operations. NetDocuments monitors access from cities such as Hong Kong, London, San Jose, Denver, and New York. Such cities will be changed from time to time to measure different issues from different areas. In the last 18 months, uptime for the NetDocuments global datacenter has been 99.9905%.

Environmental Controls

The datacenters provide controls to modulate electrical power problems such as surges, brown-outs, black-outs, etc. Both global datacenters have installed uninterruptible power supplies (UPS) for critical components along with generators with over a week's supply of fuel. They also have redundant power feeds from two different suppliers. NetDocuments datacenter is protected by a pre-action, dry pipe sprinkler system as well as gas suppression above and below the raised floor. In addition the mechanical/ electrical rooms have a pre-action, dry pipe sprinkler system and/or gas suppression.

Datacenter High Availability

The NetDocuments global datacenters were designed to achieve a high level of scalability and high-availability, supporting millions of users on a 7x24x365 basis. The NetDocuments service can be tiered into eight functional clusters for workload purposes (web, mail, domain controllers, directories, database, file servers, indexers, and application). For high availability and scalability, each functional cluster is implemented using non-stop server class machines under a highly available architecture.

The following is a summary of the global datacenter architecture and high-availability:

- Multiple Internet access providers with high speed OC3 services from four independent ISPs, all BGP-4 load-balanced, and optimized for MAE-East and MAE-West routing, and five fully redundant CISCO routers to peer with the four ISPs.
- Redundant intrusion prevention and atrium firewalls.
- Redundant network routers with multiple connections per server.

- Hardware accelerated redundant HTTPS encryption appliances.
- All servers are connected to two independent VLANs, with redundant power supplies.
- Load balancers for web servers.
- Redundant web server farms.
- Redundant mail servers.
- Redundant domain controllers.
- Redundant routers.
- Redundant back-end firewalls
- Replicated directory servers with load balancing across app servers.
- Clustered database servers.
- Redundant application servers.
- Redundant pipeline servers.
- Redundant indexer servers.
- Redundant search servers.
- Redundant query servers.
- Redundant and clustered file servers.
- Non-stop enterprise disk sub-systems (Network Appliance highly available clusters) with call-home feature, supporting mirroring, RAID-DB, and snapshots.

Trust and Transparency

Any SaaS and cloud computing platform should provide customers with detailed information about service availability and performance in real time, including information about maintenance activities and updates, service performance data, as well as making available user activity data for within the customer's.

The NetDocuments Service Status page communicates anytime there are issues that affect its users. Customers can get real time feeds by email or SMS to notify them if there are performance issues that need to be communicated. The NetDocuments Web sites are also in the Cloud with full redundancy and business continuity to ensure these sites are available and independent from the NetDocuments corporate headquarters buildings.

With a large population of customers being lawyers, financial service advisors and accountants, our customers trust NetDocuments to be the custodians of their critical corporate and firm data. NetDocuments continually monitors its procedures and policies and communicates its operations openly with its customers and partners.

NetDocuments is SAS 70 Type II as well as achieving the eTrust Safe Harbour audit. The SAS 70 standard (Statement on Auditing Standards No.70) was developed by the American Institute of Certified Public Accountants (AICPA), and is an internationally recognized auditing standard. SAS 70 designation represents that the AICPA or its designees have conducted a rigorous audit of the

NetDocuments controls and safeguards over its information technology and all related processes. SAS 70 Type II audit describes the company's internal controls at a point in time and assesses whether they were suitably described to achieve control objectives.

The TRUSTe EU Safe Harbor Seal communicates that the NetDocuments Web site has committed to protecting the privacy of EU visitors through compliance with the EU-US Safe Harbor Framework and participation in TRUSTe's Watchdog Consumer Dispute Resolution service. The EU-US Safe Harbor Framework was developed by the U.S. Department of Commerce in concert with the European Commission to provide a framework by which US companies may comply with EU privacy directives protecting the personal information of European citizens.

World-Class Security

NetDocuments security and privacy services have much higher standards than the majority of currently implemented corporate document services. Documents are fully protected from internal operators, datacenter operators, unauthorized internal users, and malicious hackers.

NetDocuments was built from the ground up as a hosted and distributed application accessible by the mobile user. For this reason, the entire Service was architected with security and privacy as its most important design principles as it relates to 1) physical datacenter security; 2) wire security; 3) operator security; and 4) document security.

Physical Security

From a physical security perspective, NetDocuments Services provide the following:

- Computer operators are not only bonded, but they also undergo a background check and FBI clearance.
- Operators can only enter the secured room accompanied by another bonded operator working in another department (neutralizing the "buddy effect").
- Biometric-based access control and an electronic security card are required before access to secured computer areas is granted (two-factor physical access authentications).
- All work performed by DP personnel are recorded in cameras, with tapes kept for at least 20 days.
- All operations, including software updates, undergo strict change-control policies.

- Physical security including parking lot access, reception, surveillance, arm guards presence, monitoring, food and water reserves, are strictly enforced.
- Disaster recovery policies are in place and tested every six months.
- The datacenter itself is a bunkered design with berms on exposed faces to give the facility an office building look. The glass used with the datacenter exceeds the standard specifications and all mechanical, electrical, and environmental equipment is monitored by UL approved alarm devices. All walls within the datacenter are slab-to-slab and the facility is inspected on an annual basis.
- NetDocuments datacenter has physical controls to protect resources based on criticality and sensitivity. The datacenter headquarters and datacenter are physically secured sites. Access to all buildings on the campus is controlled by badge reader access. A guard force is employed at all main entrance points to campus buildings and all visitors are required to sign-in and verify their identities before they are given temporary visitor badges to access internal facilities. Sign-in registers are review and archived. All visitors require escorts unless a prearranged registration process is satisfied for access that is more permanent. This prearranged registration process is as rigorous as our process for registering new employees.
- The access control system is segregated into secure zones. Besides the zones that control perimeter access (building ingress/egress), several zones are set up within campus buildings to restrict access to specific datacenter zones.

Wire Security

All possible means of securing the wires are employed to assure safe communications between the user and the NetDocuments Services.

- **Regular Penetration Test.** Regular penetration tests are conducted by third parties. This allows all parts of the wire security infrastructure to be audited regularly by non-datacenter security experts.
- **Communications Encryption.** All communications between user workstations and the NetDocuments service are encrypted using the SSL protocol. NetDocuments supports up to 128 bit encryption keys. NetDocuments realizes that sensitive information is contained not only in passwords and document contents but also in document metadata such as document names and comments, so NetDocuments encrypts all communications.
- **Hardware Encrypted HTTPS.** All SSL encryption and de-encryption at the global datacenter is performed by independent and redundant SSL hardware accelerators.
- **Intrusion Detection & Prevention.** IDS technology is deployed in front and behind the first level of firewall. Mechanisms exist to detect and stop intrusions and denial of services attacks before risking service breach.
- **Multiple Firewalls.** There are three levels of firewalls, each with different hardware and software providers, to increase security. The redundant firewalls are placed (1) in front of the web servers, (2) in front of the DMZ (between the web servers and the data), (3) and in front of engineering team's special VPNs (for application software updates).
- **Logging and Analysis.** One of the basic services associated with NetDocuments is logging of all communications to the bank and the deployment of sophisticated analysis tools to detect and identify security threads. Massive amounts of data,

logged in large Network Appliance disks are analyzed with Sun Servers by bank software security experts, using special purpose software, to identify any threads not detected with standard IDS technology.

- **Multi-Architecture Layered Security.** For a potential intruder, the work required to open a secured document is daunting. The intruder would need to do the following: (1) break into the first firewall and the intrusion detection systems, (2) penetrate the Unix encrypted hardware, (3) pass the Windows and Microsoft IIS security, (4) go through a different DMZ firewall, (5) break into NetWare and eDirectory secret store for further credentials, (6) compromise the file server security and the database security, (7) do this fast enough before the bank security people notice it, (8) and even if the document is obtained the information there contained cannot be read because NetDocuments does not store the document in the clear.

Operator Security

One of the most vulnerable areas for data processing security is within its own operators. This is very noticeable in an organization's own IT operations, where there are very little internal security safeguards. While organizations today have high consciousness against external unauthorized access and some management of internal user rights, there is typically no policies and enforcement against internal operators.

The computer room access to NetDocuments is strictly controlled and federally regulated. All bank operators are bonded. No individual can go into the computer room alone. An operator cannot even enter the computer room accompanied by another bonded operator, unless this other operator is from a different department (removes the "buddy collusion" problem). All operators undergo extensive FBI check. The security administrators do not access the computer rooms. They set security policies via remote software. The bank datacenter has 15 such security operators, who don't do anything else but manage the security infrastructure of the network, Internet access and logs. They report to the Bank Chief Security Officer, who must report to the federal regulators, and not to the CIO. They are not part of the hundreds of operators who monitor and administer the NOC and the rest of the computer rooms.

In addition, the NetDocuments service also allows separation of duties at the customer administration level for Repository and Cabinet Administrators. Repository Administrators, who have broad administrative rights for creating and deleting Cabinets, setting Profile information, defining users, and investigating activity logs, cannot view documents. Such privileges are granted generally to the Cabinet Administrators. The Cabinet Administrators cannot do the functions of the Repository Administrators.

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. They can neither reformat drives nor

physically damage the disks—both possible with physical WORM storage devices. Policy-based retention rules are the only method of purging records.

Document Security

NetDocuments requires a user to authenticate to the service before accessing any documents or other information stored in the Repository. Authentication credentials typically consist of a *username* and *password*. NetDocuments requires passwords to be at least six characters long. Passwords are not allowed to contain the user's username or any word in the name of any Repository the user is a member of. Passwords also cannot be comprised entirely or mostly of the user's initials. NetDocuments authentication sessions automatically time out if a user is inactive for 90 minutes.

- **No persistent storage of user's password.** NetDocuments does not persistently store user passwords. Instead, a hash of the password is stored with the user's account. This makes it impossible for an intruder or even a NetDocuments internal services Administrator to retrieve a user's password. User passwords are hashed and stored by the highly secured Novell's eDirectory secret store. The eDirectory also performs common password management functions such as automatically locking out a user who fails seven sequential login attempts.
- **Active Directory Single Sign-on.** NetDocuments also supports a single sign-on feature called Automated Login. A user logged into a Microsoft Active Directory domain can enable the Automated Login feature. At the time Automated Login is enabled, a public/private key pair will be generated. The private key will be stored in a secured location on the user's workstation while the public key will be stored with the user's account in the NetDocuments directory service. The next time the user accesses the NetDocuments login page from that workstation, the NetDocuments private key will be used to sign a time-stamped authentication token. This token will then be authenticated by the NetDocuments service and used to gain access to the service. This feature thus provides single sign-on functionality between Active Directory and NetDocuments. Users working from their office workstations do not have to login twice.
- **RSA SecurID® Two-Factor Authentication Support**. Customers who currently have RSA SecurID two-factor authentication from RSA (the security division of EMC) in place can use the same token to access their documents through NetDocuments as well as other existing corporate applications and networked resources. Used in conjunction with RSA Authentication Manager software, an RSA SecurID token functions like an ATM card for a company network, requiring users to identify themselves with two unique factors — something they know (a password or PIN), and something they have (e.g. an RSA SecurID hardware token) — before they are granted access to secure business information stored in NetDocuments.
- **Digital Certificate based Login.** NetDocuments supports digital certificate-based authentication. To enable digital certificate-based authentication, a user logs into NetDocuments and registers his digital certificate. Any X509.3 certificate is supported. The next time the user accesses the service; he can click the certificate-based login button on the NetDocuments login page. If the registered certificate and the corresponding private key are present on the user's workstation, the private key

is used to sign a time-stamped authentication token. This token is sent to the NetDocuments service where it is verified using the public key embedded in the user's digital certificate. If the token is valid, the user is logged into the service without having to re-enter his username and password.

To improve security NetDocuments displays a user's last login information the first time the user visits their Home Page in NetDocuments.

Document Privacy and Integrity

Document Privacy

NetDocuments offers a comprehensive set of choices for small to enterprise-level customers to customize and configure the security and access rights to documents.

- **Document Access Control**. Each document stored in NetDocuments has an associated Access Control List (ACL) for privacy and access level enforcement. Access Control Lists define which users are allowed to view, edit, share, and delete the associated document. Share rights allow users to share the document with other users (adding other users in the ACL string). Users may not grant higher rights than he or she owns. If a user does not have at least View access to a document, the document is completely hidden from that user and the user will not see the document in search results, folder listings, etc.
- **Security Groups**. NetDocuments support users groups for security enforcement. Associated with a document, cabinet, ShareSpaces, or folders are a series of users and/or groups with the appropriate access rights.
- **Physical Bonding of ACL and Documents**. NetDocuments uses a unique, patented method to store Access Control Lists in the same container as the documents they are associated with. The co-located ACL is verified in conjunction with any document access, such as view, read, and write operations. There is a huge differentiation between NetDocuments ACL enforcement technologies from all other competitors. In other systems, the ACL is stored in a database, while the documents are stored in a separate storage location. If there were problems in the database, document store, or document display operations, the wrong document could be displayed to the user. A NetDocuments patent technology physically bonds the access control and the document itself into a single container. With this patent, the NetDocuments service will always ensure proper privacy is enforced. *For additional details on this patent, please contact NetDocuments.*
- **Container Access Control.** In addition to document-level ACLs, ACLs are also imposed at higher levels. NetDocuments stores documents in logical groupings called Cabinets. One or more Cabinets can be combined into a single administrative unit called a Repository. Both Cabinets and Repositories have associated membership lists, and a user who is not a member of a particular Cabinet or Repository is unable to access any documents stored therein. Furthermore, documents can also be stored in binders (ShareSpaces) and folders, which also have ACL definitions to enforce document privacy.

- **Echoing Rules**. NetDocuments Echoing feature allows for the redundant storage of recently opened documents into a local PC folder (Echo folder) for high-availability, document integrity, and high-speed caching. However, for privacy reasons, echoing is not desirable when working on certain workstations. NetDocuments has customizable rules for enabling or disabling echoing. Administrators can disable echoing from certain Cabinets. Documents contained in certain Cabinets may merit a higher degree of privacy. Administrators can enable echoing only to certain IP addresses. For example, certain workstations in the office are enabled, and certain home users are allowed, but the rest will be blocked. If an IP address and Cabinet are allowed to echo, echoing will only occur if and only if these two additional criteria are met: (1) the particular "user" has enabled echoing and (2) enabled on that particular "workstation". If a different user accesses that particular workstation, echoing will not occur (someone else with a NetDocuments account using temporarily "my" workstation will not echo). If that particular user accesses a different workstation, echoing will not occur (accessing NetDocuments from a "foreign" workstation will not leave unintended echo footprints). Only when the four conditions are met (Cabinet, IP address, workstation, and user), will the documents be stored in the Echo folder.
- **Ethical Walls.** Ethical walls is the capability to enforce certain ACL privileges to a group of users, and being able to block even "view" privileges to others. NetDocuments allows for such restrictions by using the "N" (no access) ACL rights. This is a removal of rights to certain individuals, or sometimes called "negative security" (because it removes, as opposed to granting rights). For example, the ACL "GROUP A -VES, JOHN -N" indicates that GROUP A, which in this particular example includes John, has View, Edit, and Share privileges to certain document(s), but John, even if he is a member of the group, has no rights whatsoever (John cannot even know the document exist).
- **Profile Based Security.** NetDocuments allows for the security definition be based upon a certain Profile field value. For example, a department (or practice group) has a privacy setting: “all documents associated with certain departments will automatically have the ACL set based upon the triggered department values.” This makes data entry much easier, without having to individually set every document to the appropriate ACL.
- **Folder ACL Inheritance**. NetDocuments supports the concept of folders passing their ACL to sub-folders automatically. Folders can also pass their Profile metadata and privacy and security information to their documents (or objects).
- **Audit Trail.** Each time a document is created, edited, viewed, emailed, signed, etc., the action is automatically recorded in the document history. The history is maintained within the NetDocuments service where users cannot delete nor tamper. Each history record includes a server-derived date/time stamp synchronized with the Navy Atomic Clock. NetDocuments also supports digital signatures. Users can sign documents using any X509.3 digital certificate. The signature is stored in NetDocuments, along with the date/time the document was signed, the identity of the signer, and details of the digital certificate used to sign the document.

Document Integrity

Users have intrinsic expectations that the important documents under the care and management of NetDocuments will retain 100% of its contents, nothing more, and nothing less, as the documents travel from one location to another. Users trust the Service and its ability to resolve conflicts and errors caused by communications and hardware failures.

Users also expect that NetDocuments will help recover from user errors, either from prematurely deleting the document, or from inadvertently committing changes which later on proved to be unwarranted. To ensure the highest levels of trust on NetDocuments document integrity, the service implemented (in addition to other features described in this White Paper) the following safeguards:

- **Concurrency Control.** NetDocuments ensures that only one person can edit the document simultaneously.
- **Save locally before saving to server**. NetDocuments technology supports a cooperative synergy between servers and local workstations. The temporary file for the document edit process is the Echo folder. Any failures to upload back to the Datacenter caused for whatever reason will automatically trigger subsequent attempts to upload in the future until it successfully happens.
- **Check Sum Processing**. NetDocuments and Microsoft IE work cooperatively ensuring that bit strings transferred from the workstation to NetDocuments Servers are not dropped or erroneously switched. Hashing algorithms guaranteeing data transfer integrity is in place.
- **Transaction Integrity between Global Datacenter and Local Document Service.** The global datacenter sends documents to be replicated to the LD Service after the LD Service initiates the request. The workstation does not send documents to the LD Service to reduce complexity from every workstation to have yet another task to perform. Communication between the LD Service and the global datacenter follow strict transaction processing integrity rules, with each party ensuring that all documents being sent have been properly received.
- **Collision Handling**. Collisions occur when NetDocuments cannot resolve discrepancy issues. Collisions occur in certain cases: Hijacking -User #1 opens a document and never closes before going home for the evening. User #2 critically needs the same document and has "author" or "Administrator" rights over the document. User #2 is notified by NetDocuments that User #1 has the document opened (an email can be sent to User #1 from User #2 facilitated by NetDocuments). After warning messages, User #2 tells the Service to "force open" the document, affecting a hijacking from User #1 and thus creating a collision. NetDocuments resolves this collision by recording User #2 changes as the official version, while User #1 changes (upon his return the next day) will be recorded as a new unofficial version. User #1 is notified of the situation. Please note that the ability to "hijack" is required because sometimes users never close a document or sometimes the computer simply crashes for whatever reason and the document is never checked-in. In such cases, unofficial newer versions are never created because the person being hijacked never completes the process. In all cases document integrity is maintained. Echoing Conflicts -User #1 edits a document in the Echo folder in PC #1. User #2 edits

another copy of the same document in his/her own Echo folder in PC #2, before User #1 closes the document. The last person completing the transaction will have his/her document be classified as a new unofficial version, with a message explaining what had just happened.

- **Check-In List.** NetDocuments includes a Windows executable called the Check-in List, which maintains control over multiple documents currently checked-out from the customer's repository. This ensures continuous document integrity, even if the browser focus is not on NetDocuments (e.g., a user navigates away to another web site), even if the browser has been closed, even if Internet connection is lost, and even if the PC power has been turned off. The NetDocuments Check-in List maintains local management of all checked-out documents until such documents have been safely returned to the global datacenter.
- **Snapshots.** Users may make erroneous changes to documents and commit to such edits when closing and uploading the document. Users may request that documents be restored as of a certain past date. NetDocuments supports automatically up to 30 different backup snapshots for each document, and all of its versions. The Service keeps a snapshot every single day for the last 30 days. Recovering a document is simple. No tape backup restoration is required to restore a snapshot. This service is provided to ensure document integrity against user mistakes.
- **Recovering from Deletions**. Some DMS' prevent users from deleting documents, which forces garbage to clutter the repository, while other systems allow deletions only to find a very high number of Help Desk "restore from backup" requests. NetDocuments allows users to delete documents, and allow users to restore deleted documents, without IT help. Deleted documents maintain their ACL (authentication control list) and are placed in a Deleted Items List in the Cabinet, preventing users from cluttering the Repository and containers (Folders, Categories, and ShareSpaces). Administrators usually are the only ones who can purge documents from Deleted Items List. Users can go to the Deleted Items List and restore documents without Help Desk aid. NetDocuments Customer Service can still restore purged documents by the Administrator from the deleted folders for 30 days after the deletion took place. The NetDocuments mechanism for deletion processing helps maintain overall document integrity.
- **Virus scanning.** This is an optional feature, which, when turned on by the Administrator, ensures that no document containing a virus is stored in the repository. Internal and external users may inadvertently have a contaminated document. Although strict virus scanning may be in place for internal users in the organization's own computer operations, no one can guarantee that external users have such processes. Emails and attachments sent to NetDocuments folders may also contain a virus. The NetDocuments virus scanning feature deploys commercial grade virus signature recognition to identify any document attempting to be stored in the global datacenter. NetDocuments prevents it from being imported, quarantines it, and informs the Administrator to fix it. After security, the most important aspect of the NetDocuments service is performance. This service must be robust, fast, and reliable. Service response time is measured electronically and impartially through a series of 14 steps being performed every 5 minutes throughout a 365x7x24 period from automated monitoring agents from different parts of the world.

Compliance

NetDocuments offers a unique solution in meeting the regulatory compliance requirements because of the monitoring, archiving, policy enforcement, and retention solutions to all electronic files under the Software-as-a-Service (SaaS) model. NetDocuments not only addresses specific SEC, HIPAA and other similar requirements, but its SaaS model also provides a very cost-effective best practice solution, allowing you to focus your energy and resources on your clients and mission critical line-of-business requirements. NetDocuments delivers a solution that eliminates the need to invest in expensive hardware and software to create an in-house system, and its associated ongoing labor, maintenance, updates and disaster recovery. In addition, NetDocuments includes a fully functional document and content management service.

A highlight of significant NetDocuments benefits to customers includes:

- **Organization and preservation of electronic records.** Contents can be structured into cabinets and multi-tier folders or into powerful workspaces for clients or projects, with a sophisticated security model overlaid to define user and group access rights. The NetDocuments Service can be universally accessed from anywhere in the world through the Internet via workstations or handheld devices. Microsoft Office applications and Microsoft Outlook can be fully integrated into NetDocuments. Users can also find NetDocuments folders directly in Outlook and drag and drop emails and attachments directly into the Service.
- **WORM storage.** NetDocuments provides virtual WORM cabinets, where electronic files can be written once, read many times, but never altered or deleted. Digital records stored in WORM cabinets are tamper proof. Not even the customer's systems administrators can remove or modify such files; neither can they reformat drives or physically damage the disks.
- **Multiple storage locations.** Electronic files in the NetDocuments Service are physically stored in two off-site mirrored global data centers. Each data center is highly available with redundancy in all aspects of telecommunications, networking, hardware, security, and procedures. Disaster recovery is built-in.
- **Serialization of original and duplicates are securely filed and indexed**. NetDocuments offers best-of-breed searching technology indexing all documents, emails, attachments, images, and records in two redundant data center locations. Searching of all electronic contents and metadata (profile information) can be done in seconds. Search results can be displayed in any order, including relevancy ranking. Search capabilities include Boolean, keywords, phrases, linguistic lemmatization, and proximity functionality.
- **Retention policies and audit history**. Multiple retention policies can be defined to preserve digital records, according to the customer's needs and compliancy requirements. Different record types can be preserved for any retention period, such as 3 years, 6 years, 15 years, or indefinitely.
- **Document collaboration and sharing**. Increase client loyalty by securely sharing with internal or external users. All access to all documents is registered in history logs. Auditors and Compliance Reviewers can be granted immediate access to documents and indices upon request.

- **Third-Party Downloader Service.** For Financial Services broker-dealer firms that store documents or other records electronically, the SEC requires a third party designated with the SEC who can download the firm's archived electronic records and provide the documents to the SEC if requested. NetDocuments is set up to fulfill this service.

Scalability

One of the key technological breakthroughs of NetDocuments is our Portable Document Container Architecture (PDCA), which is the foundation of the NetDocuments massive scalability, extra-high level of security, and storage obfuscation. NetDocuments is a document service not only intended to scale in a very large single organization, but also intended to scale across multiple organizations sharing the same Software-as-a-Service infrastructure.

When NetDocuments was developed new patented technology was developed to ensure scalability. PDCA's advantage is the partitioning of document storage, metadata, security, and rules into discrete but pooled segments without the need for a single monolithic repository infrastructure.

This architecture provides true massive scalability. It removes the "umbilical cord" to a centralized database and distributes the target containers to each application server, where the local processor can manipulate and update the objects in local memory, accessing the documents themselves, the ACL security, the profile metadata, the history log, and all other objects therein contained, without utilizing the network or the central repository.

Furthermore, NetDocuments decentralizes the application servers, directory servers, storage servers, and indexing servers. If the application servers run out of capacity, additional ones are simply added. The same is true with virtually every component of this architecture. There is no central dependency upon a single sub-system, either from a software or hardware configuration. NetDocuments architecture and technology ensures an unprecedented massive scalability and high performance for users in a distributed Software-as-a-Service world.

Performance

NetDocuments continually reviews and enhances its service to ensure the highest performance in delivering web pages quickly and processing of features and transactions. NetDocuments utilizes the fastest hardware and software servers and respective software, and utilize server and local caching of data whenever feasible.

The following service response times are measured electronically and impartially through a series of 14 steps being performed every 5 minutes throughout a 365x7x24

period from automated monitoring agents from different parts of the world. Average response time is detailed below *(some pages will vary depending upon quantity of items to be displayed or size of document. The averages below are based on a common text based document and typical folder view):*

Action	Average
Go to Login Page	0.46 seconds
Login	0.47 seconds
Display Home Page	0.50 seconds
Go to Folder	0.33 seconds
View a document	0.18 seconds
Send a doc via Email	0.35 seconds
Search anywhere	0.66 seconds
Logout	0.09 seconds

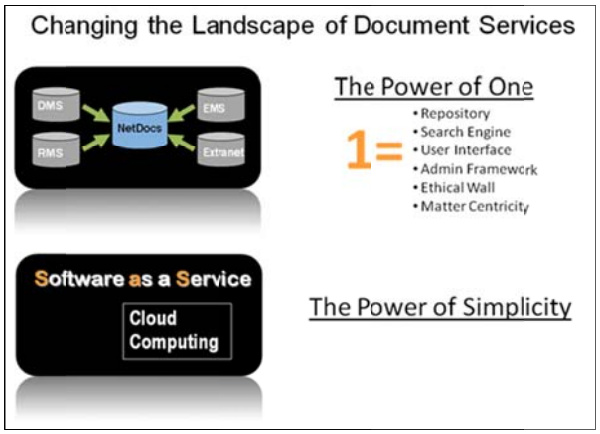
Broadband Requirements

NetDocuments optimizes performance across the Internet and is very conservative in both the amount and frequency of data transfers. In a law office document management application (where high document access and usage is prevalent), the rule of thumb is about a T1 bandwidth (1.5Mbits per second up and down) for every 200 users in the same office; or a Synchronous DSL line (500Kbits up and down) for every 40 to 50 users. The efficiency of NetDocuments is a result of its architecture. Notice the following features which minimize bandwidth:

- **Local Caching.** When opening a document, NetDocuments will attempt to get it from the local Echo folder first, unless the Echo copy is not current. This will reduce document download from the Web by a factor of 50% to 70%. It is usually the case that a document would have been most recently edited by the same user who is attempting to open it.
- **Background Upload**. When closing a document after an edit session, NetDocuments can check-in the document back to the repository. This can be done simply by navigating out of the current screen or selecting another function. The document will be automatically returned (checked-in) to the repository without the user screen being held hostage until the transfer is complete. In other words, the user may simply go to the next desired operation, while the recently edited document will be uploaded in the background.

NetDocuments – A Software-as-a-Service (SaaS) in the Cloud

NetDocuments, as a SaaS, cloud-based document and email management service, allows you the freedom to access and work on your documents anywhere and anytime, 24x7x365. Organize into project/client/matter-centric workspaces. Search the content of your Word, Excel, PowerPoint, PDF's, and emails. Have the peace of mind knowing your work is backed up and secured in world-class data centers.



An organization that deploys NetDocuments immediately has a document management, email management, collaboration, and digital records management—all within a single repository. It becomes the ***Power of One***. One set of services across all your content, one set of searching services across all your content, one set of authentication and security across all of your content, and one user interface and global access across all of your offices and content.

The NetDocuments service has been in operation since September 1999. It is a very seasoned application with a rich set of features and functionality. Managing well over 100 million documents one would think that the performance would degrade over time. The opposite has been the case. While maintaining the ability of the company to continually enhance performance, and develop within a single cloud model infrastructure, the company has achieved record results in reducing response times in Internet based document work performance. During the past four years from 2009, NetDocuments has seen a 608% document growth yet has experienced a 47% faster response time for users in accessing and processing their documents. These results attest to the value of a SaaS application fully optimized for the Internet and to service customers of all sizes across 144 countries worldwide.

For more information, contact sales@netdocuments.com or +1.866.638.3627.

NetDocuments
625 South State Street
Orem, UT 84058
www.netdocuments.com
801.226.6882

4816-5046-6057, v. 1