Security Overview: LexisNexis® Hosted Litigation Solutions

Be confident in a secure technology environment designed specifically for litigation hosting.

Introduction

Rest assured that your critical tools and information are in excellent hands when you rely on LexisNexis® Hosted Litigation Solutions. Safeguarding your litigation data and software is our top priority. Around the clock, you benefit from:

- Top-tier, high-availability data centers
- A secure, dedicated and customizable platform
- Our proactive, layered approach to robust security based on industry standards and many years of experience
- Our vigilance in keeping pace with evolving threats and adapting controls accordingly

LexisNexis applies best practices for server, network and physical security. The architecture, policies, and processes described in this document work together to assure the confidentiality, integrity and availability of data processed, stored and delivered through LexisNexis Hosted Litigation Solutions.

Table of Contents

LexisNexis®

Security Policy

The LexisNexis Security Policy is based on observed experience, common practices and guidance from industry standards, such as ISO/IEC 27001 and ISO/IEC 27002, which outlines a framework for information security management and a corresponding code of practice. LexisNexis has a wide variety of security policies in place to protect data that is hosted at a LexisNexis facility.

Physical Security

Our customers can rest easy knowing their data is hosted in secure, highly available, Tier 3 certified data centers. Our data center controls are SSAE-16 certified in the U.S. and ISO 27001/14001/9001 certified in the UK.

The LexisNexis hosting facilities generally contain the following physical security:

- Facility is enclosed by a security fencing system
- Swipe access with PIN code is required to enter main doors to the data center
- Man-trap revolving door is in place to enter from the lobby
- Data Center Security Control is staffed 24/7/365
- Closed-circuit televisions—some with pan/tilt/zoom—have cameras recording for a minimum of 30 days
- Access is electronically logged for all door openings and closings
- All hosting clients requiring access to secured areas are escorted

Storage Architecture

LexisNexis provides an enterprise-class storage solution for primary data storage capacity and secured on-site data backups for retention and restoration. Additionally, an alternate LexisNexis site is used for data replication, retention and backups via private network circuit.

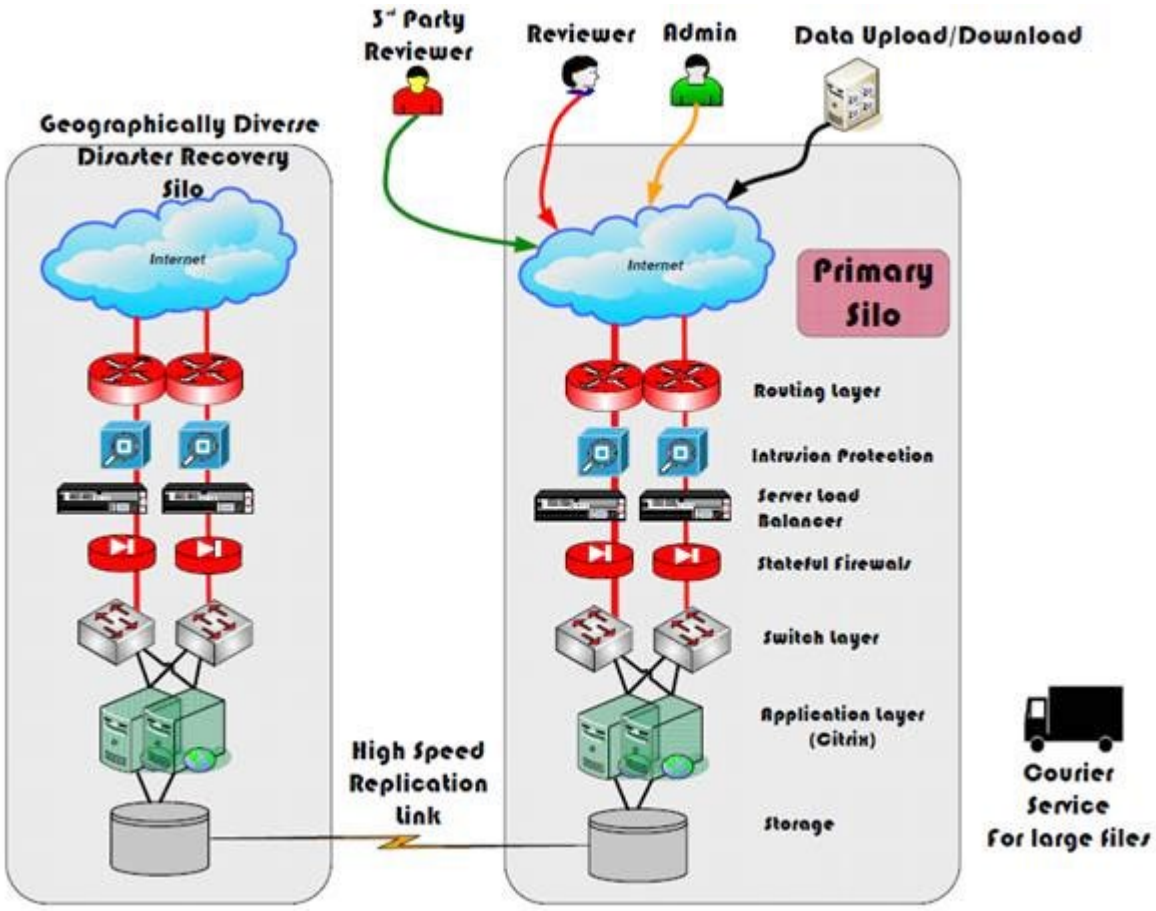
The storage solution consists of a scalable clustered storage array at the primary site and an identical clustered array at the secondary facility. The disks are configured using proprietary double-parity Raid-6 implementation to prevent data loss. Private logical partitions are used such that no information can be viewed, used or downloaded by unauthorized users.

Business Continuity Management

The standard Recovery Time Objective (RTO) is six hours and the standard Recovery Point Objective (RPO) is one hour. Local snapshot and remote mirroring capabilities allow LexisNexis to provide very fast file restoration and disaster recovery using the minimum bandwidth between storage arrays. Snapshots occur every hour. Hourly snapshots are retained for 24 hours. Daily snapshots are retained for 30 days. These snapshots are replicated to another storage array in a different LexisNexis data center where they are available for restoration, failover and disaster recovery.

Network Architecture

We deploy a default-deny, defense-in-depth strategy to deter unauthorized access. Highly available stateful-inspection firewalls on hardened security appliances protect the Internet-facing systems. Only the ports needed to provide our services are permitted. Additionally, all communication channels between the client and the server are encrypted; e.g., there are no clear-text communications across the Internet to the client desktop. Network-based intrusion prevention systems provide an additional layer of protection by actively blocking malicious traffic at the perimeter.



Each LexisNexis Hosted Litigation Solutions customer has its own virtual local-area network (VLAN), allowing only required traffic in and out and granting no access to other customer traffic. Internal firewalls separate the hosted litigation environments from the LexisNexis internal environment and other LexisNexis product offerings. Only LexisNexis staff members directly responsible for supporting Hosted Litigation Solutions are permitted access to the hosted litigation environments.

Media Handling and Data Destruction

Physical media will be received by the LexisNexis data handlers, who will follow chain-of-custody procedures, moving the media rapidly into a limited-access loading room. The media will then be attached to a data-loading workstation with direct connectivity to the environment and will be channeled through conduit to the raised floor where the servers and storage reside. When upload is complete, the media will be stored in a dedicated and secure evidence locker until a disposition request is provided. Original media is maintained and remains pristine unless otherwise instructed by the client. We return the original data or destroy the physical media once it is loaded into the system as required by the client. Our procedures call for data sanitization meeting the requirements set forth in DOD 5220 prior to destruction.

Data Transfer

LexisNexis offers a high-performance data transfer option for large volumes of data. This option is immune to network latency, resulting in consistent transfer rates that can be achieved regardless of customer location. This provides a secure transfer maintained via AES128 encryption and built-in client certificate. To ensure customer data privacy, each customer has its own isolated server and back-end storage.

Access Control

Logical access controls exist at the storage, network (LAN, WAN, SAN), operating system, database and application levels. Each customer has a dedicated domain and virtual LAN (VLAN). System usage is restricted and is enforced through measures such as access control lists (ACLs), firewall rules, IP address, and username/password. All accounts and passwords are managed via Active Directory. Each customer has its own highly available deployment of Active Directory. Authorized requestors direct the creation, maintenance and removal of customer accounts by LexisNexis support staff.

Remote Access

Secure administrative access for customer environments is accomplished using a virtual private network (VPN). Two-factor authentication can be utilized for accounts, and split tunneling is disabled. Once a customer member is logged into the VPN, that person is granted access only to systems and networks permitted for that customer.

Endpoint Security

Security advisories and monthly vulnerability scans are used to direct configuration and patch management activities in order to address risk within the environment. Industry-standard products are used to provide comprehensive endpoint protection against a wide variety of malware threats.

Management and Monitoring

LexisNexis provides a 24x7x365 Network Operations Center (NOC) to provide continuous monitoring and support of LexisNexis environments. Network, device and application alerts are reviewed, actioned and escalated as needed. Additionally, log and event data is collected, correlated and analyzed, providing the ability to quickly troubleshoot and investigate potential issues.

Change Management

The LexisNexis change management process provides governance over changes made to both shared infrastructure and the customer environments. Changes must be documented, reviewed and approved prior to implementation.

About LexisNexis

LexisNexis® Legal & Professional (www.lexisnexis.com) is a leading global provider of content and technology solutions that enable professionals in legal, corporate, tax, government, academic and non-profit organizations to make informed decisions and achieve better business outcomes. As a digital pioneer, the company was the first to bring legal and business information online with its Lexis® and Nexis® services. Today, LexisNexis Legal & Professional harnesses leading-edge technology and world-class content, to help professionals work in faster, easier and more effective ways. Through close collaboration with its customers, the company ensures organizations can leverage its solutions to reduce risk, improve productivity, increase profitability and grow their business. Part of Reed Elsevier, LexisNexis Legal & Professional serves customers in more than 100 countries with 10,000 employees worldwide.

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis products identified. LexisNexis does not warrant this document is complete or error-free. If written by a third party, the opinions may not represent the opinions of LexisNexis.

LexisNexis®