lexbe℠
eDiscovery FAST

Lexbe eDiscovery Services
Security Overview

Keep your documents, data and work-product secure in our secure, shared, cloud environment

Lexbe Online maintains state-of-the-art security to ensure that customer documents are never compromised. Data security is our top priority and our redundant infrastructure, multi-level application controls, and strong in-place and 256-bit SSL transfer encryption deliver the highest levels of protection for your legal electronic stored information (ESI).

World Class Data Center Infrastructure– Lexbe Online operates within the Amazon Web Service (AWS) cloud environment and incorporates Amazon's Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), and Elastic Block Store (EBS) technology. Amazon is a leading service provider for the infrastructure, network, and physical security layers of a cloud-based network environment. Servers are maintained in secure, limited access physically-isolated data centers, and monitored from network operating centers 24x365. AWS data center personnel do not have logical access to Lexbe applications or to the data of any Lexbe customers hosted on Lexbe Online accounts.

Industry Leading Cloud Architecture

Documents and Data Encrypted – We transmit and store your ESI using strong 256-bit (AES-256) encryption, the same technology used by Banks. Our U.S.-based data centers have successfully completed SAS70 Type II audits, and provide Service Organization Controls 1 & 2 reports published under SSAE 16 and ISAE 3402 professional standards.

High Levels of Service Maintained

You Own Your Data – Our Terms of Service disclaim any ownership interest in your and your client's documents and data.

Ownership Rights Clear

Audits and Certifications – Lexbe's data centers have successfully completed SAS70 Type II audits, and provide a Service Organization Controls 1 (SOC 1), Type 2 report, published under both the SSAE 16 and the ISAE 3402 professional standards, as well as a Service Organization Controls 2 (SOC 2) report. Additionally, our data centers have achieved ISO 27001 certification, and have been successfully validated as a Level 1 service provider under the PCI Data Security Standard (DSS).

Independent Validation

Proactive Network Intrusion Monitoring – We operate redundant firewalls to protect our servers from potentially malicious network traffic. We also use Network Intrusion Detection Service (NIDS) technology to monitor network traffic, and to detect, report and respond to anomalies which are indicative of a network-based attack. This may involve taking proactive counter-measures when a network attack is detected, including denial of service (DOS) attacks and other potential malicious traffic or incursions at the network layer.

Intrusion Risks Managed

Reliability and Backup – We configure all servers and networking components in a redundant configuration for persistent reliability. Our uptime over the last 5 years exceeds 99.995% and we provide customers a 99.99% uptime guarantee. All customer data is stored redundantly in multiple separate data centers and synching downloads occur daily. In a disaster, we are configured to be able restore client data from remotely stored back-ups. Clients additionally can periodically download their own files and data for an additional level of protection, if desired.

Redundant Backup and Recovery Protocols