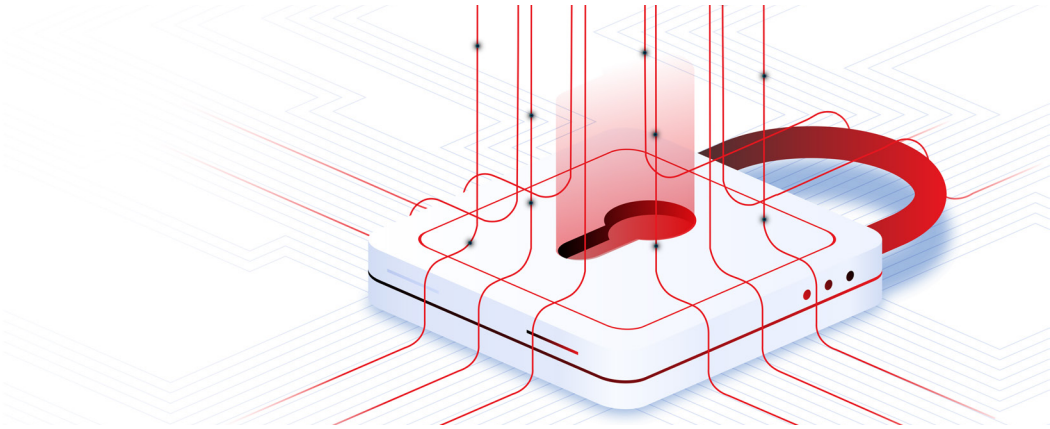
Lexis Create
Security Overview



LexisNexis Legal and Professional (LN L&P) provides quality, cutting edge and secure products to our customers. There is a dedicated application security team that works with product development, data protection officers and operations teams to ensure security controls are in place throughout the product lifecycle. This security overview of Lexis Create provides answers to some of the frequently asked questions about security and how LexisNexis is protecting our customers and their data.

POLICIES, STANDARDS AND GUIDELINES

LexisNexis has strict company-wide security policies, standards and guidelines that detail the necessary security controls and configurations that ensure all systems and data managed by LexisNexis remain secure. These policies are reviewed and updated regularly, considering changes in legal, regulatory, and operational environments, as well as to address new and emerging threats. Employees are required to complete computer-based training upon hire and periodically thereafter covering topics to include our security policies and practices, code of ethics, and data privacy.

PRIVACY

LexisNexis complies with the regulatory obligations in the various regions and countries where we operate and where our customers reside. View our up-to-date privacy policy for more information.

APPLICATION SECURITY PROGRAM

This program sets the requirements for standard security controls across all applications and products and monitors compliance with those requirements.

- Lexis Create code undergoes static application security testing (SAST) prior to being allowed to be pushed to production. Software Component Analysis (SCA) is performed as part of the CI/CD pipeline. Penetration testing is also performed on the solution.
- Due to information security policy, security tests results are not shared with customers. The application security team is available to discuss any specific security questions a customer and covered by an NDA
- Quality gates are in place to prevent unsecure code from being introduced to production.
- The application security team works with development teams to resolve vulnerabilities regardless of the source in accordance with established remediation timelines based on criticality.

AUTHENTICATION

We offer two authentication mechanisms. Firstly, we provide secure user authentication with a strong password policy. We also use federated Single Sign On using SAML 2.0.

DATA & INFRASTRUCTURE SECURITY

To the extent that Authorized Users provide their personal data to LN L&P during account registration or otherwise, the parties acknowledge that such information will be processed by LN L&P as a controller in accordance with applicable data protection laws. For more information on how LN L&P protects data privacy, see our global LexisNexis privacy statement available to all customers. To the extent that LN L&P acts as a processor of Personal Data on behalf of Customer, LN L&P will comply with the LN L&P data processing addendum. Lexis Nexis is a data controller.

Customer data, i.e. when the user uses the snippet functionality to save a clause within their document, is stored only in the Cloud. Lexis Create only deletes customer data at the direction of the customer. At rest, data is encrypted at the volume using AES 256-bit encryption. Lexis Create allows access to data only by authorized support personnel with permissions on a need to know (principle of least privilege). LexisNexis gathers analytical statistics regarding usage of application functions but does not process any customer data specifically.

In Lexis Create, a user's uploaded document is stored temporarily in the application's active memory during the user's Lexis Create session. The text and extracted data from user's document are deleted when the user's session ends. The process followed is that a user's document is scanned by the proof-reading engine; rules get applied locally; the results are displayed and are shown in the add-in. The document's content is stored in local memory and cached whilst the rule engine is processing rules. Once the rule engine finishes processing the document's content is cleared from the memory. If the user document changes and is re-scanned, then the above process is run through again. No content is transferred to the server or leave the local machine.

The citations feature in Lexis Create analyses the document locally and extracts out the citations. Lexis Create sends the citations to the LexisNexis Citation Service to retrieve the full text citations so it can be displayed in the add-in. No documents (i.e., content) is transferred to the server.

The snippets feature in Lexis Create stores snippets in the cloud so that they can be retrieved by the user later. Stored snippets can be explicitly shared with other team members.

Lexis Create does not pass any data to a third party. To improve our recommendations over time, we primarily rely on internal data analysis, using publicly available, filed documents as the input documents. We have expert data scientists and attorney analysts who evaluate the relevance of the results and provide feedback that leads to further improvement in the technology behind Lexis Create. We also conduct regular customer research as part of our ongoing development process.

SUPPORT

For more information please contact your Sales Representative or call 1-800-387-0899.