Lexis+ AI™

Lexis+ AI™ Security Information

Security, Privacy and Trust: Our Promise

LexisNexis® Canada prioritizes security in everything we do. Our products are developed with a philosophy that puts customer data protection at the core.

Our comprehensive data protection program ensures that we safeguard your valuable information. We've assembled a dedicated team of application and security experts who work closely with our product development and operations teams to ensure every product meets rigorous, audited standards.

Experience industry-leading security and cutting-edge technology with LexisNexis solutions. Count on us to safeguard your most valuable assets while delivering exceptional performance.

Use the navigation links below to explore our commitments to protecting your data.

DEDICATION TO REGIONALIZATION

LexisNexis is committed to supporting our customers' data residency expectations. Lexis+ AI is deployed in a manner that helps customers meet regional data handling preferences, particularly those that prioritize maintaining data and processing activity within Canada.

Customer interactions with Lexis+ AI are processed through infrastructure hosted in Canada and the EU. While the AI application runs in Canada, our Large Language Models operate exclusively within secure, private cloud environments in Canada and the EU. These environments are protected by the same rigorous LexisNexis security controls that apply across our global platform.

Importantly, customer data is retained and processed only in these designated regions, with no transference to other geographies.

This regional deployment model is designed to provide confidence to organizations that require strict control over data movement and residency, ensuring that Lexis+ AI operates in alignment with their contractual and client-based obligations.

DATA HANDLING

Your Prompts

- Your conversations are purged after 90 days or when deleted by the user, whichever comes first.
- Conversation history is stored in a secure environment and encrypted at rest using AES-256.
- LexisNexis' Large Language Model partners are contractually bound not to train their models on your data.
- Our cloud providers maintain logs for support and troubleshooting purposes, but they do not have access to user prompts.

Your uploaded Documents

- Your documents remain under your control and can be deleted by removing the session conversation thread. The system will also purge documents after 10 minutes of inactivity or if you navigate to a new window or browser tab.
- Documents are retained only for the duration of an active session.
- Conversations related to uploaded documents are purged after 90 days or upon user deletion, whichever comes first.

Privacy

Privacy by Design principles are embedded throughout the development process, with compliance oversight to ensure LexisNexis solutions adhere to applicable privacy and data protection laws. All employees undergo data protection training as part of standard onboarding, with annual mandatory refreshers. Confidentiality and data protection clauses are included in all employment and service contracts.

ENCRYPTION

All Lexis+ AI customer data (prompts and documents) is encrypted at rest using AWS Key Management Service and **AES-256** encryption. All internet traffic in transit is also encrypted using **TLS 1.2.** Each customer request is processed independently and generates a separate transaction within the generative AI system.

AUDITS & POLICIES

LexisNexis engages an independent third-party auditor to perform an annual SOC 2 Type 2 examination of Lexis® and Lexis+, based on the Trust Services Principles of Security, Availability, Processing Integrity, Confidentiality, and Privacy. New assets for Lexis+ AI will also undergo regular SOC 2 examinations.

LexisNexis maintains a **robust** set of information security policies that enable us to respond efficiently to potential **threats**. Our incident response plans — **updated and tested periodically** — cover technical, administrative, business, and executive escalation procedures. We also retain external firms to provide expert guidance as needed.

SECURITY & ACCESS CONTROL

Network security controls are implemented based on the principle of least access. These controls protect against unauthorized access and traffic interception, restricting both inbound and outbound traffic as well as internal communications between systems. Where necessary, private endpoints are used to securely access cloud services and ensure the security of associated transactions.

Access to company networks is restricted to corporate-managed devices and protected by multi-factor authentication. Authorizations follow the principle of least privilege. Privileged accounts are granted based on job function, approved by management, and subject to regular access reviews. Access is automatically revoked upon termination.

The LexisNexis Vendor Management Program conducts vendor **security and background checks** during the procurement process. Vendors are evaluated using a risk-based approach that considers factors such as access to customer or company data, system integration, and the criticality of services provided.

We perform regular vulnerability and penetration testing using internal tools and third-party firms to validate our defenses. Automated internal and external scans provide continuous visibility into new risks. All findings are tracked centrally to ensure proper prioritization, and remediation efforts are coordinated accordingly.

ARCHITECTURE

Lexis+ AI (Canada) is deployed and maintained using the same security architecture, reviews, audits, and validation as Lexis+TM Canada and our other products. Generative AI capabilities have been engineered and deployed to meet our high-level security standards across regions in Canada and the EU, with a key focus on protecting and segmenting customer activity. Our security team continues to be actively engaged in all aspects of the engineering and deployment of Lexis+ AI.

High-level architecture flow:

1. A user's prompt, query, or document is securely transmitted via **TLS 1.2** to Lexis+ servers.

2. The prompt is parsed for intent and divided into discrete queries by an embeddings model to retrieve relevant information from our content store.
3. The prompt and content response are securely sent via **TLS 1.2** to our private Large Language Models.
4. A grounded, generated response is returned to the user in Lexis+ AI.
5. User prompts and responses are retained for up to 90 days in a secure, **AES-256**-encrypted database. Documents are **purged** after **10 minutes of session inactivity**.
6. Vendor models do not have access to our models or services. Our architecture **prevents these organizations from logging or training models** based on users' conversations.
7. Our model vendors maintain logs for **support and troubleshooting purposes** but do not have access to users' prompts.

FAQ'S

Will my entries into the tool be used to train the Lexis+ AI model?

No. LexisNexis does not use customer data to train or fine-tune our Large Language Models. Users have individual control over their prompt history and may delete it at any time. For more details, please review our privacy policy.

Will Lexis+ AI utilize third-party systems to process my data?

Yes. LexisNexis uses third-party AI technology providers to ensure Lexis+ AI incorporates the most advanced generative capabilities. All third-party providers are vetted through our security review processes.

The models are deployed exclusively in protected, private cloud environments that are part of the secure LexisNexis infrastructure. These environments are governed by LexisNexis security controls that apply across our platform. The models are used solely by LexisNexis and are not accessible to the public or other companies.

All models utilize dedicated, encrypted, and authenticated connections that meet or exceed our high security standards. Customer data is always encrypted and remains under the control of LexisNexis.

What are your encryption standards?

All Lexis+ AI customer data (prompts and documents) is encrypted at rest using AES-256 and in transit using TLS 1.2.

Can LexisNexis employees see my chat queries?

Only a restricted group of authorized product support experts may access customer usage data, and solely for product support and technical troubleshooting. Customer identity is pseudonymized to protect user privacy.

What about my uploaded documents, are they retained?

Uploaded documents are stored in a temporary AWS cache for the duration of your session. They are automatically purged after 10 minutes of inactivity, or users can delete them by removing the session conversation thread.

Can firm administrators limit the use of Lexis+ AI to certain features or users within the firm?

Yes. Firm administrators can manage individual user access to Lexis+ AI and may temporarily disable features in response to information security concerns.

Where can I find documents and reports related to your audits and policies?

Audit reports and policy documents are available upon request. Please contact your account team for access.

Is my Lexis+ AI data shared with other LexisNexis services?

No. Customer data is only available within the specific product context in which it was entered. It is not shared with other LexisNexis products unless explicitly authorized and communicated.

OTHER MATERIALS

LexisNexis Legal & Professional Data Privacy Principles

Responsible Artificial Intelligence Principles at RELX

Your Peace of Mind Is Our Priority

In-depth InfoSec Document - Available Upon Request

Detailed Architectural Drawings - Available Upon Request

CONTACT

security@lexisnexis.com

privacy.inquiries@lexisnexis.com