Sound privacy, security and compliance practices are essential to the well-being of your business. We incorporate best practices in these areas into the solutions that we offer customers in business, legal, corporate, government and non-profit organizations. Because we place a strong, competitive focus on privacy, security and compliance and because we integrate each of these components into our business model, you can trust that LexisNexis® is a partner who is dedicated to protecting your interests. Mitigating risk for customers and consumers while delivering best-in-class solutions and services is our priority.

- We strive to employ best-in-industry safeguards so that the information you need is accessible and reliable.
- Our safeguards are designed to protect you against improper access and impermissible use.

All of this means that when you choose LexisNexis solutions, you’ll know we are taking steps to help you ensure that your business and your identity are safe, secure and protected. Our risk-management program is designed to provide you with the peace of mind you need to focus on what is most important: driving results for your business.

Seven key areas differentiate LexisNexis in privacy, security and compliance:

1. **Risk-Mitigation Framework**
   - LexisNexis promotes the responsible use of information by employing a risk-management framework for privacy, information and physical security, and compliance. The framework is based on ISO 27002 and includes administrative, physical and technical safeguards designed to reasonably protect the privacy, confidentiality and security of personal information collected from or about consumers. Proprietary customer credentialing criteria and continuous security controls are also key components of the LexisNexis privacy, security and compliance framework.
2. Data Security
To deliver a consistently high standard for data security, LexisNexis utilizes controls across systems. In addition to utilizing more than 150 internal controls designed to prevent unauthorized access, LexisNexis conducts back-end suspicious activity monitoring to detect and respond to anomalous account activity. We also work proactively to identify and resolve potential vulnerabilities in our systems.

3. Credentialing
LexisNexis credentialing and re-credentialing processes verify that access to data is granted to legitimate individuals or entities and for permissible purposes. Our credentialing and re-credentialing processes include: (1) customers, (2) LexisNexis employees and (3) vendors/third parties. Through these processes, LexisNexis helps to mitigate the risk of fraud by verifying and re-verifyng LexisNexis employee background information, customer and vendor business credentials and permissible regulatory and legitimate business purposes for accessing information products, systems and data.

4. Policies, Standards and Guidelines
LexisNexis has implemented strict policies, standards and guidelines throughout the company that govern data access, protection, transport, restriction, retention, deletion and classification for customers, employees and vendors. Policies, standards and guidelines are reviewed and updated regularly—in light of changing legal, regulatory and operational environments, as well as to address new and emerging threats—and communicated to our customers, employees and vendors on an ongoing basis.

5. Audit and Compliance
A robust and detailed program of audit and compliance is in constant operation to review and test policies, standards and guidelines, as well as legal and regulatory requirements, to assess whether they are working effectively and efficiently and being adhered to by customers, employees and vendors, as appropriate. The LexisNexis audit program includes in-house and third-party audits as well as independent assessments.

6. Accountability
At LexisNexis, privacy, security and compliance are integrated into the business model. To us, accountability means fulfilling our obligations to customers, consumers, employees, stakeholders and shareholders, specifically including privacy, security and compliance.

7. Training, Communication, Outreach and Transparency
We are committed to keeping both internal and external stakeholders informed and up to date about what LexisNexis is doing to respect privacy and keep information secure. Employees receive mandatory training with assessment, and customers, employees and vendors are informed of their obligations relating to privacy, security and compliance. Dedicated LexisNexis personnel are available to assist consumers with general inquiries and requests.

Our team of experts is always willing to furnish further information about what we’re doing to provide you with the peace of mind you need to focus on your business. For more information about privacy, security and compliance at LexisNexis, please visit www.lexisnexis.com/privacy

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Other products and services may be trademarks or registered trademarks of their respective companies. © 2017 LexisNexis.