

LexisNexis® Security and Privacy: An Overview of How We Protect Information

Here are just a few examples of how law enforcement, Homeland Security, and commercial and legal customers apply LexisNexis® products in a positive way to find solutions to real-life problems:

- Reducing consumers' financial losses
- Reducing fraud
- Reducing the risk of terrorist attacks
- Helping to find missing children

LexisNexis products that use public records and non-public information are invaluable tools for these kinds of applications.

The LexisNexis Group is committed to delivering products that benefit consumers, the government agencies that serve and protect them, and the organizations they do business with.

We are committed to vigilantly protecting the security of information as well as the privacy of consumers and customers from potential misuse. That commitment is why LexisNexis has implemented and continually enhances its comprehensive security and privacy policies.

The LexisNexis Commitment to Security and Privacy

Our commitment to security and privacy is integrated into our business model and business strategy.

LexisNexis Group has established a Privacy, Security and Compliance Department to oversee and enhance privacy, security and compliance organization-wide.

All LexisNexis employees receive mandatory and continuing security and privacy education as well as regular internal communications.

As part of our work with clients such as financial institutions and government agencies, we are required to regularly undergo full-scale, third-party security audits. LexisNexis has successfully completed more than 100 third-party security audits since 2001.

LexisNexis Group supports a number of efforts to help shape the development of effective policies and best practices in the information services industry. For example, LexisNexis was a founding corporate partner of the **Center for Applied Identity Management Research** (www.caimr.org). CAIMR is a non-profit corporation comprised of thought leaders from government, corporate and academic organizations who share a common interest in the multi-faceted aspects and critical challenges of identity management. CAIMR is based at Indiana University with a research agenda focused on identity theft and fraud, cyber crime, computer crime, travel and immigration document fraud, data breaches, and terrorism and national security. Government partners include the Department of Defense, U.S. Marshals Service, United States Secret Service and the Federal Bureau of Investigation, along with a number of other academic and corporate partners including Cogent Systems, Visa, Wells Fargo, and Lockheed Martin.

Memberships in the U.S. Secret Service Electronic Crimes Task Force and the FBI InfraGard organizations are additional examples of the LexisNexis commitment to constantly measure and address today's changing threats.

Security

Security includes the various mechanisms LexisNexis implements to protect the LexisNexis information systems and the data accessed through its databases from potential unauthorized access.

Maintaining security is a dynamic process. It requires continuously evaluating and adjusting security procedures to address new threats. LexisNexis continues to reassess and adapt its systems to respond to evolving threats to privacy and information security.

LexisNexis® Security and Privacy:

An Overview of How We Protect Information

LexisNexis has multi-layered systems for information technology, information security and physical security to ensure the availability, confidentiality and integrity of data, using industry-standard access control software and methods. LexisNexis information and system security professionals regularly refine these processes to address new threats.

Privacy

Privacy includes protecting consumer information in the LexisNexis databases and systems and verifying that it is accessed by authorized subscribers for appropriate uses.

LexisNexis customers have different access to different types of LexisNexis information depending on their need, or permissible use, for specific types of information, and on LexisNexis policies. LexisNexis customers requesting access to sensitive data must be authenticated and verified before being allowed access to LexisNexis data. New customers and existing customers requesting data class upgrades go through a multi-step application, approval and validation process, including site visits where appropriate. This process independently verifies the customers' business and their purpose for accessing sensitive information.

Additionally, LexisNexis protects privacy through:

- Restricting the display of full Social Security numbers and Driver's License numbers to businesses and entities that have verifiable identities and have a substantiated need for sensitive personal information, and who are permitted such access pursuant to LexisNexis policies;
- Requiring password-strength standards that help ensure customer ID and password security;
- Implementing a Phishing Defense Program which helps LexisNexis identify potentially compromised customer credentials and disable their access to sensitive data; and
- Restricting from where customers may access sensitive information.

Audit and Compliance

LexisNexis employs a program of internal and external audit and compliance to test the controls and safeguards that are implemented through its privacy and information security framework. A program of audit and compliance also helps compliance with applicable laws, regulations, agreements, and internal policies and procedures. LexisNexis undergoes regular external audits and

assessments and conducts various internal audits to test the following:

- FCRA customer permissible purpose
- Consumer sampling verifying purpose
- Non-FCRA customer business purpose
- Customer usage of data
- Reseller compliance
- Mandatory training compliance
- Web-site privacy policies compliance
- Public representations
- Regulatory compliance
- Policy compliance

For More Information

Please visit

<http://www.lexisnexis.com/privacy/data-privacy-principles.aspx>
to view the LexisNexis Data Privacy Principles and learn more about Privacy, Security, and Compliance at LexisNexis.