THOMSON REUTERS CLEAR® INFORMATION SECURITY SUMMARY

Thomson Reuters maintains its reputation for providing reliable and trustworthy information through a variety of means, not least of which is a comprehensive information security management framework supported by a wide range of security policies, standards, and practices.

This document explains Thomson Reuters approach to information security and data privacy for CLEAR. It is designed to answer questions our customers regularly ask to satisfy security requirements.

Thomson Reuters information security customer statement is available upon request.

ONLINE INVESTIGATION SOFTWARE

Thomson Reuters CLEAR is designed to meet the unique needs of your investigations and fraud prevention programs. CLEAR streamlines your research by bringing relevant content into a single working environment online, through batch files or through an API. The online customizable dashboard and intuitive interface saves time by allowing you to search data and view results in a way that matches how you work.

CLEAR software makes it easier to locate people, businesses, assets and affiliations, and other critical information. With its vast collection of public and proprietary records, investigators are able to dive deep into their research and uncover hard-to-find data.

PHYSICAL AND ENVIRONMENTAL SECURITY

- Diverse set of strategic data centers hosting the technology infrastructure
- Strategic Data Centers maintain ISO 27001 and ISO 9001 certification
- Physical access controls include restricted access, security guards, and video surveillance
- Senior management approval for all physical access provisioning, including visitors
- Visitor registration requires presentation of government-issued identification

ACCESS CONTROL

- Query data is stored securely and mechanisms are in place to prevent unauthorized access
- Only authorized personnel have access to workspace data

continued ...

INFORMATION SECURITY SUMMARY

RESILIENCE

- Thomson Reuters has established a global, structured framework based on industry-accepted standards which are designed to support recovery should a disruptive incident occur
- Data center features include key resilience measures including two separate power supplies, separate UPS systems, multiple 2-MW diesel generators, HVAC, batteries, fire suppression, CCTV monitoring, and more
- Redundant application servers and disaster recovery tools are implemented
- Data servers are backed up regularly

POLICIES AND STANDARDS

- Information Security Policies and Standards are reviewed and approved by senior management annually
- Employees and contractors are required to review and acknowledge the Information Security Handbook
- Employees and contractors are required to acknowledge and review the Code of Business Conduct and Ethics

TRAINING AND AWARENESS

- All employees and contractors who require logical access to Thomson Reuters systems complete security awareness training annually

VULNERABILITY ASSESSMENTS

- Internet-facing systems are scanned for vulnerabilities on a repeating basis
- Penetration testing is conducted by a third-party tester
- Application code is regularly scanned by industry-standard third-party security tools

APPLICATION SECURITY

- Thomson Reuters has a formal change management process that is performed by authorized personnel
- Thomson Reuters utilizes secure practices within the agile methodology as part of the Software Development Life Cycle
- All development staff are required to complete security training, with a focus on best practices and OWASP Top 10 security risks. The security learning program promotes secure design, development, and testing best practices
- CLEAR uses highly trained technical support staff who are available on-site – 24/7/365
- CLEAR has a SOC2 Type 2 report, which covers operational control systems that follow the predefined trust services principles and criteria
- CLEAR conducts an annual third-party assessment based on Payment Card Industry Standard

MULTI-FACTOR AUTHENTICATION

- CLEAR software uses multi-factor authentication and also offers two-factor authentication (OnePass) for secure user login

ENCRYPTION

- All interaction with CLEAR software occurs inside secure sessions
- CLEAR data is encrypted in transit
- Data and metadata in CLEAR is encrypted in transit and while at rest

For more information, contact your Thomson Reuters representative or visit:
legalsolutions.com/clear

The intelligence, technology and human expertise you need to find trusted answers.

the answer company™
THOMSON REUTERS®

© March 2019 Thomson Reuters S052452/9-17