CLEAR®

Information Security Summary

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
• Our commitment to a secure operating environment is demonstrated by our ongoing certification program of our data centers’ information security management systems (ISMS) to ISO/IEC 27001:2013.
• Thomson Reuters data center facilities are secured by computer-managed access control systems with security guards monitoring entrances.
• Visitor registration requires presentation of government issued identification. Visitors are required to sign in at building entrances and must have escorts within the buildings as well as appropriate badges.
• Access is recorded, documented, and monitored across our data centers. Multi-level security access is required for access to restricted areas, e.g., ID cards, electronic access control incorporating proximity card readers, pin numbers, and/or biometric devices.
• Access to delivery and loading areas is controlled and monitored, and deliveries and access are only allowed in those controlled areas.

Policy and Standards
• Thomson Reuters manages a set of information security policies and standards which outline information security and risk management principles that apply to our people, processes, and technology practices.
• Our policies and standards are closely aligned with the International Organization for Standardization (ISO/IEC 27002:2013) and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).
• 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 review and acknowledge the Code of Business Conduct and Ethics.

Access Control
• CLEAR® query data is stored securely, and mechanisms are in place to prevent unauthorized access.
• CLEAR® employs Thomson Reuters’ identity and access controls and regularly reviews administrative access to enterprise resources, product environments, and applications.
• Role-based access controls ensure appropriate access rights, permissions, and segregation of duties.

Vulnerability Management
• Manual Penetration Tests (MPTs) are conducted by a third party tester on an annual basis.
• Application code is regularly scanned by industry standard third party security tools.
• Internet facing systems are regularly scanned for vulnerabilities.
Secure Authentication

- CLEAR® software uses multi-factor authentication and offers two-factor authentication (OnePass) for secure user login.
- CLEAR® users must be authenticated to the CLEAR® web-based application with a unique CLEAR® userID and password.
- Single Sign-On (SSO) configuration is also available via Secure Authentication Markup Language (SAML).

Encryption

- All interaction with CLEAR® software occurs inside secure HTTPS sessions.
- CLEAR® data is encrypted in transit using TLS supported protocols.
- CLEAR® data at rest is encrypted with AES encryption.

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.
- 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

End Point Security

Servers

- Led by a team of experienced security professionals, advanced anti-malware, network intrusion detection systems and intrusion prevention systems have been deployed across our fleet of devices designed to monitor and defend the environment.

Employee Workstations

- Managed internal services endpoints at Thomson Reuters are required to be protected by an up-to-date version of the standard malware protection solution. Signature deployments are required at least daily to internal technology services assets.
- Thomson Reuters has a data leakage protection program in place worldwide, subject to local law and regulation and where legally permissible.

For more information, contact your Thomson Reuters representative.

Data Privacy and Compliance

- Thomson Reuters Privacy Statement can be found online at: https://www.thomsonreuters.com/en/privacy-statement.html.
- CLEAR® obtains a SOC 2 Type 2 report annually, a third party assessment conducted on application security controls, which covers operational control systems that follow the predefined trust services principles and criteria.

Training and Awareness

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

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.
- Production data center features include key resilience measures, such as separate power supplies, UPS systems, diesel generators, HVAC, batteries, fire suppression, CCTV monitoring, biometric authentication, and more.
- Redundant application servers and disaster recovery tools are implemented.
- Data servers are backed up regularly.