THOMSON REUTERS

CLEAR

Information Security Summary

Product Documentation

This document explains Thomson Reuters' approach to information security and data privacy for **CLEAR**.

Protecting our customers' information is at the core of our Information Security strategy. Thomson Reuters maintains its reputation for providing reliable and trustworthy information through a variety of means, including a comprehensive information security management framework supported by a wide range of security policies, standards, and practices.

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 can dive deep into their research and uncover hard-to-find data.

Our Employees

- All Thomson Reuters directors, officers, employees, and contractors ("employees") are subject to the Thomson Reuters Code of Business Conduct and Ethics which sets forth the laws, rules, and standards of conduct that apply to our employees in all the countries where we do business.
- Thomson Reuters employees must complete pre-employment background screening checks and comply with confidentiality depending on the country and position at issue, to the extent customary and permitted by law.

Training and Awareness

- Employees with access to Thomson Reuters systems are required to complete mandatory information security and privacy training on an annual basis.
- Specialized training is delivered by Thomson Reuters to particular groups of employees as necessary.
- Thomson Reuters conducts regular enterprise-wide phishing simulation exercises to all employees.
- Thomson Reuters also partners with third-party vendors to provide training resources for all skill levels through customized internal programs.

Policy and Standards

- Thomson Reuters manages a set of information security policies and standards designed to provide 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 are required to acknowledge and review the Thomson Reuters Code of Business Conduct and Ethics annually.

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.

Resilience

- Thomson Reuters has established a global, structured framework based on industry accepted standards 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.

Physical and Environmental Security

- Thomson Reuters' commitment to a secure operating environment is demonstrated by our ongoing ISO/IEC 27001:2013 certification program of our data centers' information security management systems (ISMS).
- Thomson Reuters data center facilities are secured by computer-managed access control systems with security guards monitoring entrances.
- In the event an on-site visit is granted by Thomson Reuters, 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.

Access Control

- Thomson Reuters uses role-based access controls to ensure appropriate access rights, permissions, and segregation of duties.
- CLEAR employs Thomson Reuters' identity and access controls and regularly reviews administrativeaccess to enterprise resources, product environments, and applications.
- CLEAR query data is stored securely, and mechanisms are in place to prevent unauthorized access.

Secure Authentication

- CLEAR software uses multi-factor authentication and offers two-factor authentication via OnePass for secure user login.
- 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 at least TLS 1.2 supported protocols.
- CLEAR data at rest is encrypted with at least AES 256-bit key encryption.

Application Security

- Thomson Reuters has a formal change management process that is performed by authorized personnel.
- Thomson Reuters has an established process around changes which are considered and tested prior to implementation.
- CLEAR operational and code changes are included in the change control process, for example database changes, network connectivity changes, implementation of new hardware, and changes to existing hardware.
- Thomson Reuters utilizes secure best practices within the agile methodology as part of the Software Development Life Cycle.
- Development staff participates in a security learning program promoting secure design, development, testing and security industry best practices.
- Password complexity is enforced, and a captcha system is used to defend against brute force attacks.
- CLEAR uses highly trained technical support staff who are available-24x7x365.

Vulnerability Management

- Manual penetration tests are conducted annually by a third-party tester.
- Application code is regularly scanned by industry standard third-party security tools.
- Internet facing systems are regularly scanned for vulnerabilities.

Copyright © 2022 Thomson Reuters. All rights reserved.
Thomson Reuters may modify this document at any time
to reflect changes to the law or changes to our services.

THOMSON REUTERS®

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.
- Detection and alerting mechanisms record external access attempts and attempts to interrupt or degrade the service.
- Web servers are configured to disable unnecessary services, activate/deactivate guest accounts and require complex passwords.

Employee workstations

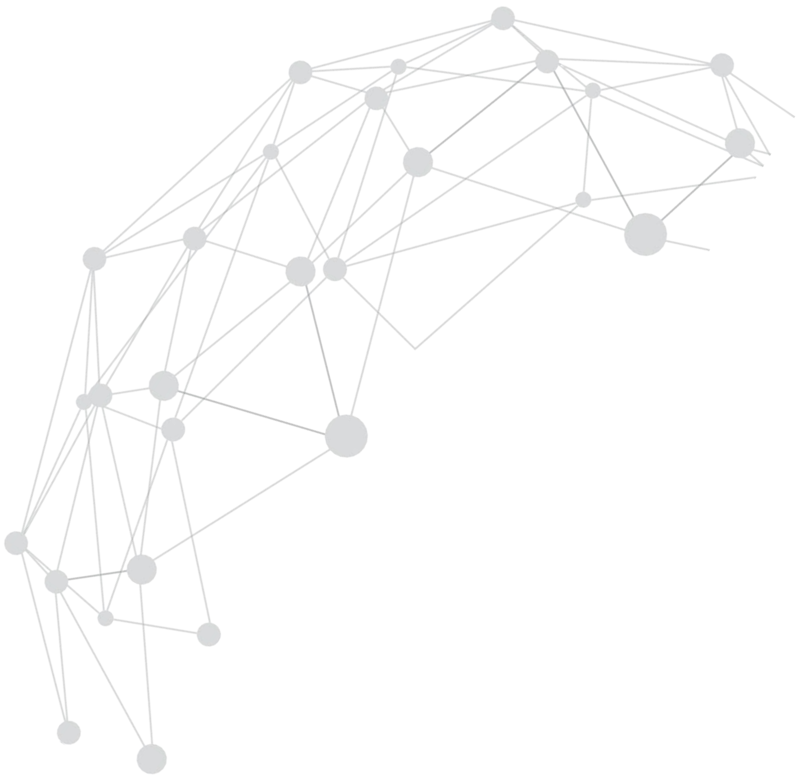
- Managed internal services endpoints at Thomson Reuters are required to be protected by an up-to-date version of the standard malware protection solution. Signature deployments are required at least daily to internal technology services assets.
- Thomson Reuters has a data leakage protection program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

Security Operations

- Thomson Reuters follows a 24x7x365 Security Operations model, with a global response footprint and a main Cyber Fusion Center located in Richmond, Virginia.
- Analytics, sensors, software agents, vulnerability scanners, and application white-listing tools are deployed across data centers to help detect, disrupt, or deny malicious activities, including spoofing, hijacking, and distributed denial of service (DoS).
- A dedicated team of security analysts provides continuous monitoring and analysis of the latest security threats to help identify and defeat malicious activities.

For More Information

- About Corporate Governance visit our Investor Relations site online at: https://ir.thomsonreuters.com
- Read about our products online at: https://thomsonreuters.com
- Our Procurement Guide describes customer contracting policies and is available online at: https://www.thomsonreuters.com/en/resources/thomson-reuters-procurement-guide.html
- Contact your Thomson Reuters Representative or contact us online at: https://www.thomsonreuters.com/contact-us



Copyright © 2022 Thomson Reuters. All rights reserved.
Thomson Reuters may modify this document at any time
to reflect changes to the law or changes to our services.