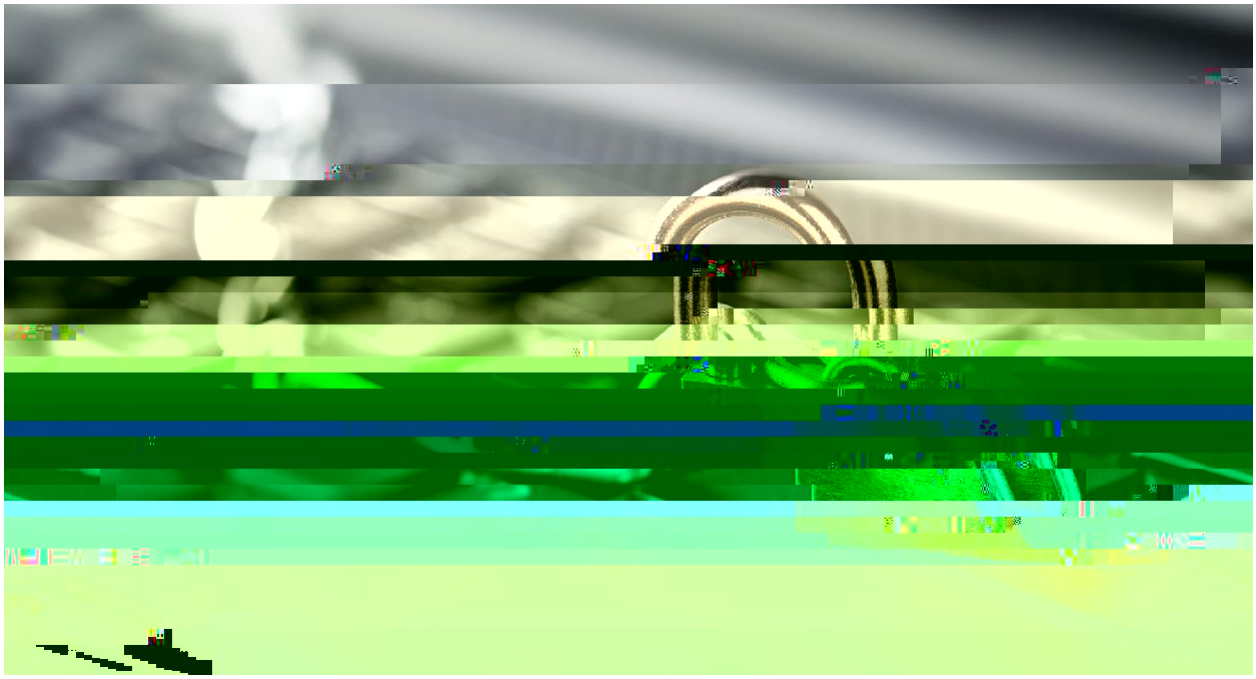
[redacted]

March 2023

Thomson Reuters is a leading provider of business information services. Our products include highly specialized information-enabled software and tools for legal, tax, accounting, and compliance professionals combined with the world's most global news service – Reuters. For more information on Thomson Reuters, visit tr.com and for the latest world news, reuters.com.

We maintain our 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.

This document explains Thomson Reuters' approach to information security and risk management.



White Paper

Thomson Reuters has dedicated resources focused on improving information security practices who strive to identify risks to our information assets and to guard against unauthorized access, loss, or misuse. As part of managing such risks, we use a variety of controls, security devices, monitoring tools, and threat models to analyze our systems and network.

Thomson Reuters has built an enterprise risk management framework that incorporates cyber security risk assessments conducted on a semi-annual basis.

Product and technology teams engage with information security subject matter experts to conduct architecture reviews, security penetration testing, vulnerability scans, application security testing, and technical compliance reviews to identify and mitigate security risks within Thomson Reuters.

Thomson Reuters has built an enterprise risk management framework that incorporates cyber security risk assessments conducted on a semi-annual basis. The enterprise risk framework includes governance procedures and management oversite for accepting risk associated to cyber security.

Cyber Risk Analytics and Security Ratings

Thomson Reuters is committed to meeting external cyber risk analytics and security ratings footprint as indicated by third-party scanning partners such as BitSight. We leverage a risk-based approach and a defined process to continuously monitor and address findings identified by BitSight as well as our internal processes and tools.

Thomson Reuters maintains a Data Protection Services (DPS) program designed to minimize the cybersecurity, business and legal risk associated with intentional or unintentional data loss. The DPS Program accomplishes this by using data loss prevention technologies, engaging employees on proper data handling, and providing incident response on data handling violations.

Data Disclosures

Thomson Reuters takes its responsibilities as both a data controller and data processor very seriously and maintains a process to manage requests from individuals who wish to exercise their rights of access, as well as correction, amendment, and deletion.

More information can be found in the Thomson Reuters Privacy Statement which is available online at: https://www.thomsonreuters.com/en/privacy-statement.html.

Data Encryption

Thomson Reuters is committed to protecting our data and that of our customers and has employed data encryption in accordance with industry standards. Our encryption policies and standards are designed to preserve the confidentiality, integrity, and availability of data and to prevent unauthorized access, use or disclosure. Additionally, the policies and standards are designed to protect data while in transit or at rest.

Data Storing and Processing

Thomson Reuters uses several geographically dispersed data centers that are aligned to support our global businesses, including partnerships with multiple cloud service providers. Additionally, we leverage country-specific regions and hosting sites for some areas that are sensitive to latency and are aligned to contractual, legal, and regulatory requirements.

Patch Management

Thomson Reuters' patch management standard follows industry best practices and product security principles which adhere to specific requirements wherein patches are communicated, rated, and deployed in an effective manner. The standard requires that technology teams deploy security patches based on their importance, and within specific time frames. We also employ forced patching protocols to mitigate unknown threats. Where required, additional Endpoint Protection security controls may be implemented to provide mitigation against known threats.

Endpoint Protection

Thomson Reuters takes the threat from malware to its networks and its customers very seriously and uses a variety of methods to prevent, detect and eradicate malware.

Our comprehensive endpoint protection strategy features antivirus scanners to protect against uploading and downloading malicious content. We deploy a combination of endpoint and antivirus solutions to prevent and detect both server and workstation environments to identify and prevent malicious code from reaching Thomson Reuters. The virus signature files are updated automatically, and our system administrators can also manually upgrade antivirus software as soon as important updates are available. Any update made to the virus software is validated and tested before being applied.

Cyber Intelligence

Thomson Reuters utilizes a range of commercial and open-source intelligence sources to enable our teams to continuously monitor, analyze, and mitigate potential cyber threats to the company. This intelligence includes indicators of compromise, attacker tactics and techniques, and changing motivations and targeting across threat groups. As new threat details are identified, we work to ensure our network and endpoint detection and prevention technologies are updated to better defend against these evolving threats.

The company also participates in strategic threat sharing forums and partnerships, which provide increased visibility into the latest threat trends observed across industries to which Thomson Reuters is aligned.

Thomson Reuters has an established resilience strategy to ensure our continued ability to serve our customers, and to protect our people and assets. Our Business Continuity Plan (BCP) prepares us to respond and recover from disruptive incidents including but not limited to natural disaster, pandemics, transit shutdowns. The BCP itself is company confidential and

Our Business Continuity Plan prepares us to respond and recover from disruptive incidents such as natural disaster, pandemics, transit shutdowns.