March 2024

Thomson Reuters AI Governance and Security Program

Thomson Reuters™

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 an 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.

Contents

"The classification is based on the intended purpose and scope of the AI model and/or the system in which an AI model's output will be embedded. Depending on the ethics harm classification, relevant ethics controls for that specific AI model are identified."

Artificial Intelligence (AI) at Thomson Reuters

Thomson Reuters has a long history of innovation in the Artificial Intelligence (AI) space as far back as 1975. Our position on the security of AI includes a multi-faceted approach to protecting traditional as well as generative AI model(s) integrated as features within our product portfolio. Our approach aligns to multiple regulatory and best practice frameworks, as well as following Thomson Reuters' Data and AI Ethics Principles:

1. Thomson Reuters' use of data and AI are informed by our Trust Principles.
2. Thomson Reuters will strive to partner with individuals and organizations who share similar ethical approaches to our own regarding the use of data, content, and AI.
3. Thomson Reuters will prioritize security and privacy in our use of data throughout the design, development, and deployment of our data and AI products and services.
4. Thomson Reuters will strive to maintain meaningful human involvement, and design, develop and deploy AI products and services and use data in a manner that treats people fairly.
5. Thomson Reuters aims to use data and to design, develop and deploy AI products and services that are reliable, consistent and empower socially responsible decisions.
6. Thomson Reuters will implement and maintain **appropriate accountability measures** for our use of data and our AI products and services.
7. Thomson Reuters will implement practices intended to make the use of data and AI in our products and services understandable.
8. Thomson Reuters will use employee data to ensure a **safe and inclusive** work environment and to ensure employee compliance with regulations and company policies.

Use of LLMs and Data in Training AI Models

Our use of Large Language Modules (LLMs) is governed by Thomson Reuters' principles, frameworks, policies, and standards. We maintain governance policies and standards designed to minimize use of sensitive data in AI models, with escalated reviews by a Model Ethics Committee within Thomson Reuters that evaluates the use of sensitive data within an LLM. Thomson Reuters has also built an internal LLM and AI solution for internal utilization and is actively driving employees to use the internal application for product development.

Data and AI Governance

The Data and Model Governance team, part of the Data and Analytics organization within Thomson Reuters, is responsible for driving and embedding an industry-leading, data-driven culture across Thomson Reuters. Their core focus is to engage across the enterprise to uplift capabilities in data and model stewardship, governance, ethics, and risk management. This is accomplished through a range of policies and standards, derived templates, governance-related tasks, as well as guidance and training material. Defining clear accountability structures helps embed the responsible use of data and AI models in existing processes and lifecycles.

Data AI Governance in Practice

Model Identification/Registration: AI models intended for a business purpose are required by policy to be registered in the centralized AI Registry, part of the Enterprise AI Platform. Model Registration is designed to enable a 360º view of Thomson Reuters' associated product, status, development, and deployment platforms.

Data Impact Assessment

The Data Impact Assessment (DIA) is an early-stage identification of data and AI model governance risks, privacy, and ethics considerations, linked to internal policies and standards. When reviewing DIAs, ethically sensitive use cases are flagged early to enable appropriate mitigation of AI ethics harm throughout the entire model lifecycle. The classification is based on the intended purpose and scope of the AI model and/or the system in which an AI model's output will be embedded. Depending on the ethics harm classification, relevant ethics controls for that specific AI model are identified. These controls are derived from the Data and Model Ethics Standards, including, but not limited to: Human Oversight, Transparency in Data Management and Model Development, Fairness in Data Management and Model Development, Automated Decisions, and Ethics by Design.

Model Risk Assessment

The Model Risk Assessment is used to proactively plan the level of risk-driven rigor, resource prioritization, and additional support required for a given AI model. It assesses the impact to Thomson Reuters of an AI model's failure across various dimensions, including financial impact, reputational impact, and customer impact.

Model Design, Development and Documentation

The Model Design and Development process defines expectations for design, data processing or analysis, development, training, and testing for AI models used by Thomson Reuters. Our Model Documentation Template brings structure, responsibility, and accountability to the management of AI models. It covers the AI model lifecycle, and captures key information around business purpose, model design, training data, model deployment, as well as third party AI model details where applicable.

“Thomson Reuters operates a global information security organization that is aligned with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).”

Model Monitoring

Model Monitoring and services are there to support early remediation in case of AI model degradation. The Model Monitoring captures model performance metrics, frequency of automated ad-hoc performance tracking, baselines, thresholds, notifications, and actions.

Model Decommission

Our Model Decommission process is also in place to aid in keeping our AI Registry up to date by assessing if an AI model should be decommissioned. If an AI model is no longer in use, or superseded by a more recent version, it should be set as inactive.

Information Security Overview

Thomson Reuters operates a global information security organization that is aligned with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). We strive to continuously enhance our capabilities to prevent, detect, and respond to threats, as protecting our customers’ data is at the core of our strategy.

Thomson Reuters has a global team of certified security and privacy subject matter experts dedicated to the security of Thomson Reuters products and services. This extended team is committed to our Information Security Risk Management (ISRM) Program, which is endorsed by the Thomson Reuters Executive Committee.

Security Defense in Practice

Thomson Reuters strives to prioritize security in the use of data throughout the design, development, and deployment of data and AI products and services, as stated by Thomson Reuters’ Data and AI Ethics Principles. A defense-in-depth approach is taken to secure products and AI models. This approach aligns to multiple regulatory requirements and best practices and will continue to evolve as new regulatory guidance is published.

Product Security

Thomson Reuters has a defined Software Development Lifecycle that aligns to secure best practices with the ability to perform security architecture reviews for the product and infrastructure. Regular internal and external vulnerability scans and code scans are completed to support the identification and remediation of security flaws.

Platform Security

Secure infrastructure configurations are based on industry best practices for configuration management. Technologies such as mobile device management, antivirus, endpoint detection and response, least privilege functionality, vulnerability scanning, phishing defense, and encryption are designed to maintain a secure compute environment on which our products are hosted.

Data Security

At Thomson Reuters, protecting data is at the core of our Information security strategy. We use a data classification structure that sets forth the security controls outlined in a Data Security Policy for the management of data throughout its lifecycle. This includes creation, storage, use, sharing, archival and destruction along with data handling guidance.

Access Controls

Thomson Reuters employs identity and logical access security controls to the enterprise network and infrastructure, product environments, and applications for employees, contractors, and third-party suppliers. Thomson Reuters has designed identity and access controls to adhere to various established industry standards and best practices including principle of least privilege, segregation of duties, unique IDs, strong password creation and management, multi-factor authentication, and privileged access management. We use privileged access management designed to secure administrator access at the system level, which includes the use of multi-factor authentication. Privileged credential checkout is managed within the enterprise vault solution to help ensure privileged accounts are vaulted, rotated and auditable for accountability and traceability.

Security Defense and Response

Thomson Reuters utilizes a SIEM (Security Information and Event Management) solution for centralized log collection and monitoring. A 24x7 follow-the-sun Security Operations Center (SOC) monitors the SIEM and uses security tools and services to protect our customers, data, assets, and operations around the globe. A tiered incident management and escalation model exists with documented response practices. Coordination of incidents is cross-functional and includes representation across Thomson Reuters designed to manage the handling of incidents.

Vendor Cyber Risk Management

Thomson Reuters Vendor Cyber Risk Management Program performs due diligence on vendors and partners to manage appropriate controls to protect Thomson Reuters data and customer data. Third party vendors are contractually obligated to comply with Thomson Reuters standards. Assurance assessments are conducted for vendors on a periodic basis.

Data Privacy

Thomson Reuters employs a dedicated Privacy Office that is responsible for implementing and overseeing a global Privacy Program that supports Thomson Reuters' compliance with applicable privacy and data protection laws. Our Privacy Program is founded upon the Privacy Management Framework (PMF), formerly known as the Generally Accepted Privacy Principles (GAPP) framework, established by the Association of International Certified Professional Accountants (AICPA). As it relates to AI, members of the Thomson Reuters Privacy Office also collaborate closely with our Data and Analytics team, customer segments, and other business lines so that privacy issues and compliance risks in AI are understood and addressed in line with the requirements of the PMF and our standards of conduct. Additional information about how we handle personal data and how we address our responsibilities where we act as a data controller can be found in the Thomson Reuters Privacy Statement.

Shared Responsibility

The responsibility for Data and Model Ethics lies with all Thomson Reuters employees. The Thomson Reuters Data and Model Ethics team works collaboratively with stakeholders across the enterprise to manage the delivery of trusted data and AI models. Thomson Reuters also maintains a cross-functional Ethics Advisory Committee as an internal oversight function to monitor new AI legislation and ethics safeguards for incorporation into AI solutions.

Employee Training

In-person as well as self-paced training is made available for Thomson Reuters employees supporting Data Governance, Model Governance, and Data and Model Ethics. The goal is for employees supporting the design, development, and deployment of AI solutions to have access to education to help ensure the use of data and AI by Thomson Reuters are informed by the Data and AI Ethics Principles.

Thomson Reuters personnel, including employees and contractors with access to the Thomson Reuters systems, are required to complete an annual, mandatory Thomson Reuters Information Security and Privacy training course. These employees and contractors also participate in quarterly phishing exercises, and additional specialized training is provided as needed.

For More Information

- About Corporate Governance visit our Investor Relations site.
- View or download our Code of Business Conduct and Ethics.
- About our products, visit our website at: https://thomsonreuters.com/.
- About customer contracting policies, see our Procurement Guide.
- Contact your Thomson Reuters account representative or contact us online.

Thomson Reuters™