the answer company™
THOMSON REUTERS®

Thomson Reuters Data Security Addendum (May 2020)

This Data Security Addendum (the "***Addendum***") shall apply to the products and services set forth in the agreement to which it is attached and is fully incorporated therein. In the event of a conflict between the terms and conditions of this Addendum and the agreement, the terms and conditions of this Addendum shall take precedence. Customer shall be the same as Customer, Client, or you; and Thomson Reuters shall mean the same as us, we, TR or Thomson Reuters, as the terms may be used in the applicable agreement. As used herein, any references to "Customer Materials" means information provided to Thomson Reuters by Customer which Thomson Reuters is required to host, use or modify for the provision of a Thomson Reuters' service or product.

1. INFORMATION SECURITY PROGRAM

1.1 Thomson Reuters will maintain an information security program designed to protect the confidentiality, integrity and availability of Customer Materials. The program will include, but is not limited to, the following components:
- (i) Information security policy framework
- (ii) Program documentation
- (iii) Auditable controls
- (iv) Compliance records
- (v) Appointed security officer and information security personnel

1.2 Thomson Reuters will establish and maintain information security policies, standards and guidelines designed to protect the confidentiality, integrity and availability of Customer Materials hosted in services which shall include the following:
- (i) Policies to restrict access to Customer Materials only to authorized Thomson Reuters personnel and subcontractors.
- (ii) Policies requiring the use of unique user ID's and passwords.
- (iii) Policies requiring secure connections to the internet to have commercially reasonable controls to help detect and terminate unauthorized activity prior to the firewall maintained by Thomson Reuters.
- (iv) Policies requiring performance of regular vulnerability assessments of Thomson Reuters LAN, WAN and critical application and network components.
- (v) Policies for the use of anti-malware and patch management controls to protect against virus or malware infection and exploitation of security vulnerabilities.
- (vi) Policies and standards for the use of auditable controls that record and monitor activity.

1.3 Thomson Reuters will train and communicate to personnel defined information security principles and information security policies and standards.
- (i) Thomson Reuters personnel shall be trained in information security practices and the correct use of information processing facilities to minimize possible security threats.
- (ii) Security awareness training attendance reports shall be maintained in the constituent's personnel file or other compliance tracking tool.
- (iii) Thomson Reuters personnel shall be required to report any observed or suspected threats, vulnerabilities, or incidents to the designated point of contact.
- (iv) Information security personnel shall be made aware of information security threats and concerns and shall be equipped to support the Thomson Reuters information security policy in the course of their normal work.

1.4 Thomson Reuters will manage personnel access to systems supporting the services to be granted on a need-to-know basis consistent with assigned job responsibilities.

1.5 Thomson Reuters shall have comprehensive business continuity plans. These plans shall be tested and approved by Thomson Reuters management on a periodic basis.

1.6 Thomson Reuters shall maintain a program for vendor risk assessment and will maintain contractual provisions with the vendor requiring vendor to maintain adequate security policies and procedures.

1.7 Thomson Reuters shall maintain a formal plan for incident response to promptly address suspected or confirmed breaches of Customer Materials or systems supporting the services.

2. DATA SECURITY CONTROLS

2.1 Application Strategy, Design, and Acquisition. Thomson Reuters shall:
- (i) Inventory applications and network components that support provision of hosted services and assess their business criticality.
- (ii) Perform Thomson Reuters standard security compliance review for acquired or developed applications.
- (iii) Review critical applications at least annually to ensure compliance with industry and commercially reasonable security standards.

2.2 Anti-Virus and Anti-Malware. Thomson Reuters shall:
- (i) Implement and configure anti-virus and anti-malware software for regular signature updates.
- (ii) Implement threat management capabilities to protect systems holding or processing Customer Materials.

2.3 Network Security. Thomson Reuters shall:
- (i) Configure network devices (including routers and switches) according to approved lockdown standards.
- (ii) Govern and monitor changes to network security controls (including firewalls) using change management standards.
- (iii) Segregate data center networks into separate logical domains with the network security controls approved by security personnel.

2.4 Web and Application Security. Thomson Reuters shall:

(i) Maintain commercially reasonable security measures for internet-accessible applications.

(ii) Implement a change management process for documenting and executing operational changes in services and applications.

(iii) Implement a documented process for the management of encryption keys including rotation of encryption keys.

2.5 Audit & Compliance

(i) Thomson Reuters will establish and adhere to policies that comply with applicable laws and standards. However, Thomson Reuters is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to software and content providers in the legal and tax & accounting market segments. Thomson Reuters does not determine whether Customer Materials include information subject to any specific law or regulation and compliance with any such law or regulation is the sole responsibility of the Customer.

2.6 Physical and Environmental Security

(i) Thomson Reuters services systems will be housed in secure facilities protected by a secure perimeter, with industry standard security barriers and entry controls.

(ii) Thomson Reuters facilities will be physically protected from unauthorized access, damage and interference.

(iii) Access to the facilities will be logged and logs will be securely maintained.

(iv) Procedures will be maintained for visitors and guests accessing Thomson Reuters facilities.

(v) Thomson Reuters equipment will be physically protected from security threats and environmental hazards.

3. SECURITY QUESTIONNAIRES AND ASSESSMENTS

3.1. Once per 12 sequential calendar months, Customer may request Thomson Reuters in writing to complete an information security and physical security assessment questionnaire. Thomson Reuters agrees to respond to such questionnaire as soon as commercially reasonable. Customers who purchase multiple products under one or more agreements shall coordinate requests into a single questionnaire per the 12 calendar month period

3.2. To the extent Thomson Reuters performs and makes available to Customers an independent third-party assessment or certification with respect to that service (e.g., SOC 2), upon Customer's request, Customer may review an available summary of the results of such security assessment for the services containing Customer Materials.

4. NOTIFICATION OF SECURITY BREACH

4.1 Thomson Reuters will, without undue delay, notify Customer of an actual breach or an unauthorized use or disclosure that directly and adversely impacts the security and confidentiality of Customer Materials ("Security Breach"). In the event of any such Security Breach, Thomson Reuters shall perform a root cause analysis to identify the cause of such Security Breach and shall, upon request, provide to Customer a report detailing the cause of such Security Breach.

4.2 Notification of a Security Breaches will be delivered to the Customer by any means Thomson Reuters selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information.