Last Modified: November 3, 2023

information processing facilities to minimize possible security threats;

(ii) Applicable Thomson Reuters personnel will be instructed to report any observed or suspected threats, vulnerabilities, or incidents to our Security Operations Center; and

(iii) Thomson Reuters information security personnel will be made aware of reported information security threats and concerns and will support the Thomson Reuters information security policy in the course of their normal work.

1.4 Thomson Reuters will be responsible for its personnel s compliance with the terms of the Agreement and with Thomson Reuters standard policies and procedures. Thomson Reuters will maintain a disciplinary process to address any unauthorized access, use, or disclosure of Your Data by any Thomson Reuters personnel.

1.5 Thomson Reuters will maintain a formal plan for incident response to promptly respond to suspected or confirmed breaches of Your Data in accordance with regulatory and legal obligations.

1.6 Thomson Reuters policy with respect to

perimeter, with generally accepted industry standard security barriers and entry controls for providers of similar services, including:

(i) Such Thomson Reuters facilities will be physically protected from unauthorized access, damage, and interference;

(ii) Access to such facilities will be logged and logs will be maintained;

(iii) Procedures will be maintained for visitors and guests accessing such Thomson Reuters facilities; and

(iv) Thomson Reuters will employ physical safeguards designed to protect Thomson Reuters Services systems from security threats and environmental hazards.

2.7 Security Testing and Patching.

(i) Thomson Reuters will perform security testing for common security coding errors and vulnerabilities against systems holding or processing Your Data in line with generally accepted industry standards.

(ii) Thomson Reuters will regularly scan systems holding or processing Your Data for security vulnerabilities.

(iii) Thomson Reuters will follow a commercially reasonable and industry standard security patching process.

2.8 Exchange, Transfer, and Storage of Information.

(i) Thomson Reuters shall ensure that all account usernames and authentication credentials are stored and transmitted across networks and protected with a minimum of 128 AES encryption. Thomson Reuters shall not store user credentials in clear text under any circumstances. Your Data shall be encrypted at a minimum of 256 AES when in transit and at rest. Thomson Reuters will also use encryption for Your Data being transmitted across the public Internet or wirelessly, and as otherwise required by applicable laws. Thomson Reuters will hold such encryption keys in the strictest of confidence and limit access to only named individuals with a need to have access.

(ii) Your Data will not be stored or transported on a laptop or any other mobile device or storage media, including USB, DVDs, or CDs, unless encrypted using a commercially reasonable encryption methodology. All electronic data transfers of Your Data by Thomson Reuters will be transmitted via SFTP or other commercially reasonable encrypted form.

2.9 Penetration Testing, Monitoring, Vulnerabilities.

(i) Thomson Reuters or an appointed third party may periodically perform penetration testing on the Thomson Reuters systems supporting the Services. Upon written request, Thomson Reuters shall make available to Customer a summary on the outcome of such relevant penetration testing or an executive summary of the penetration testing results.

(ii) Thomson Reuters will monitor the relevant Thomson Reuters information systems for security threats, misconfigured systems, and vulnerabilities on an ongoing basis.

access controls to help ensure appropriate access rights, permissions, and segregation of duties.

2.11 Segregation of Data. Thomson Reuters agrees that Your Data hosted within the Services in a production environment is maintained so as to preserve logical segregation of Your Data from data of others.

2.12 Data Removal, Deletion and Destruction. If not otherwise set forth in the applicable Agreement

background checks may include identification verification, prior employment verification, criminal background information, global terror/sanctions checks and education verification.