HighQ Information Security Controls

1. GENERAL

1.1 These HiqhQ Information Security Controls ("Information Security Controls") apply when you purchase a license to use or access HighQ as set out in the applicable Order Form. "You", "your" and "Customer" mean the client, customer or subscriber identified as such in the order form and "we", "our" and "Thomson Reuters" mean the Thomson Reuters entity identified in the order form and, where applicable, its affiliates. Any capitalized terms used in these Information Security Controls not defined herein shall have the meaning set forth in the applicable Agreement.

1.2 If there is a conflict between these Information Security Controls and any other document forming the Agreement, the order of precedence is as follows: order form and any product terms therein, these Information Security Controls, annexes, schedules and general or master terms and conditions.

2. INFORMATION TECHNOLOGY SECURITY PROGRAM

2.1 We shall implement and maintain a security controls program that is designed to comply with applicable laws, accepted standards for the industry in which we operate, and the Agreement and is designed to address security and confidentiality concerns, protect against anticipated or actual threats or hazards to security or integrity, as well as being designed to prevent unauthorized access, acquisition, destruction, use, modification and/or disclosure of Your Content.

2.2 We shall have a security and privacy policy that provides guidance to our personnel that is designed to protect the confidentiality and integrity of Your Content which addresses the following:

2.2.1 instructions regarding the steps to take in the event of a compromise or other anomalous event;
2.2.2 delegation and assignment of responsibilities for security and privacy;
2.2.3 management oversight for the policy and its deployment;
2.2.4 means for managing security and privacy within the enterprise;
2.2.5 policies and procedures for data confidentiality and privacy and data protection and access thereto;
2.2.6 handling of confidential information; and
2.2.7 planning for incident response in the event of a security incident or unauthorized disclosure of any confidential information.

2.3 Our security program shall include the implementation of administrative, physical and technical safeguards that are designed to protect Your Content and are consistent with accepted standards for the industry in which we operate, and we shall take commercially reasonable efforts designed to ensure that all such safeguards, including, without limitation, the manner in which personally identifiable information is collected, accessed, used, stored, processed, disposed of and disclosed by us complies with applicable laws, as well as the Agreement.

2.4 We agree that we shall maintain a vendor risk assessment program and will maintain contractual obligations with our vendors requiring that they maintain adequate security policies and procedures. We will take commercially reasonable efforts to procure that our subcontractors that deliver the HighQ products under the Agreement shall do so in accordance with good industry practice.

3. SECURITY BREACH PROCEDURES AND OBLIGATIONS

3.1 As used herein, a "**Security Breach**" means any act or omission that compromises either the security, confidentiality or integrity of Your Content.

3.2 Each party shall provide the other with the name and contact information of an employee who shall serve as the primary security contact in resolving obligations associated with a Security Breach.

3.3 Following our notification to you of a Security Breach, the parties agree to reasonably cooperate with each other as necessary during the investigation of the matter. We shall perform a root cause analysis of any Security Breach, and upon your request will provide a report detailing the cause of such Security Breach.

4. DISASTER RECOVERY

4.1 If our hosting site for the HighQ product becomes inoperable, inaccessible or subject to a material disruption, we will use commercially reasonable efforts consistent with good industry practices to switch to the alternate site within the same geographical area, as quickly as reasonably practicable.

5. SECURITY QUESTIONNAIRES

5.1 No more than once every twelve (12) sequential calendar months, you may request in writing for us to complete an information security and physical security questionnaire. We agree to respond to such questionnaire as soon as commercially reasonable.

6. SECURITY TESTING

6.1 We shall conduct penetration testing of the HighQ product at least annually. Upon your reasonable request, and subject to confidentiality obligations that may be owed to our clients or vendors, we shall make available for your review, copies of the executive summary report of such tests. You shall treat such reports as our confidential information under the Agreement.