Thomson Reuters Acceptable Use Policy

1. INTRODUCTION

Thomson Reuters has formulated this acceptable use policy ("Policy") in order to encourage the responsible use of Thomson Reuters' networks, systems, services, websites and products (collectively "Thomson Reuters Managed Services") by our customers and other users (collectively "Users") to enable us to provide a safe operating environment for our Users.

This Policy sets out:

- the behaviours required from Users when using Thomson Reuters Managed Services
- certain prohibited actions; and
- possible actions by Thomson Reuters if Users fail to meet those minimum standards.

The Policy is designed to protect both User and Thomson Reuters from any claims from third parties that the User's use of the Thomson Reuters Managed Services is inappropriate or damaging to such third parties.

By using the Thomson Reuters Managed Service the User agrees to be bound by this Policy. Thomson Reuters reserves the right to modify this Policy in its discretion at any time. Such modifications will be effective when posted. Any use of the Thomson Reuters Managed Services after such modification shall constitute acceptance of such modification.

Simply exercising good judgement and common sense whilst using the Thomson Reuters Managed Services should enable Users to remain within the purview of acceptable conduct as described in this Policy. The actions prohibited and the minimum standards set out in this Policy are not a complete list. If you are unsure about any contemplated action or use please contact your Thomson Reuters account team.

2. UNACCEPTABLE USE

2.1 Illegal Use. Users are prohibited from using Thomson Reuters Managed Services to commit or aid in the commission of any crime, fraud, or act which violates law, rules or regulation in and of any locality, state, commonwealth, province, nation, or international unions and federations.

2.2 Prohibited Content. Thomson Reuters Managed Services may not be used to transmit, distribute, disseminate, publish, or store any materials, data or information ("Content"):

(a) in violation of any applicable local, national, or international law or regulation;

(b) infringing any patent, trademark, trade secret, copyright, or other intellectual property right of any third party;

(c) consisting of defamatory, libellous, abusive, menacing, indecent, obscene, harassing, threatening or encouraging bodily harm, destruction of property, or infringement of the lawful rights of any party as defined under applicable law;

(d) violating the privacy or exploiting publicity of any in violation of local, national, or international law, rules or regulation;

(e) containing software viruses, worms, Trojan horses, time bombs, cancelbots, or other harmful or deleterious computer code, or any computer code, files, or programs designed to disrupt, destroy, disable, invade, gain unauthorized access to, or corrupt, observe, or modify without authorization, any data, network transmissions, software, computing or network devices or telecommunications equipment;

(f) consisting of unsolicited or unauthorized advertising, promotional materials, bulk email, or chain letters; or

(g) generally, in a manner that may expose Thomson Reuters or any of its personnel to criminal or civil liability.

2.3 Wire Tapping/Eavesdropping. The unauthorized interception or monitoring of any third party Content, other data or messages transmitted over Thomson Reuters Managed Services is strictly prohibited.

2.4 Unauthorized Access. Thomson Reuters Managed Services may not be used to gain unauthorized access to any computer, network, Content, other data or messages for any purpose, including, but not limited to:

(a) retrieve, alter, or destroy Content or data;

(b) probe, scan or test the vulnerability of a system or network; or

(c) breach or defeat system or network security measures such as authentication, authorization, confidentiality, intrusion detection, or monitoring.

2.5 Impersonation and Forgery. Thomson Reuters Managed Services shall not be used for the purposes of:

(a) impersonating any other person, party or entity by adding, removing, or altering header information of network, email, or other messages transmitted over the Thomson Reuters Managed Services;

(b) transmitting messages that have been electronically signed using a fraudulently obtained public key certificate or with a forged electronic signature; or

(c) using Thomson Reuters Managed Services to commit any other form of forgery or illegal or unauthorized impersonation.

2.6 Malicious Disruption. Use of Thomson Reuters Managed Services for interfering with or disrupting (i) the business operations, service, or function of Thomson Reuters, the Thomson Reuters Managed Services, any other Users, or any computer, host, network, or telecommunications device or (ii) the legitimate use of Thomson Reuters Managed Services by any client is strictly prohibited.

This prohibition requires that no User use the Thomson Reuters Managed Services to make deliberate attempts to overwhelm an application, computer system, network device, or network.

2.7 Security Auditing, Assessments, Penetration Tests. No security audits, assessments, and penetration tests of the Thomson Reuters Managed Services shall occur without the express written consent of Thomson Reuters

2.8 Misuse of Supplier Termination Equipment. The use of Thomson Reuters Managed Services to tamper with or attempt to gain unauthorized access to *Third Party Network Termination Equipment* is strictly prohibited.

Thomson Reuters will cooperate with appropriate law enforcement agencies and other parties involved in investigating claims of illegal or inappropriate activity. Thomson Reuters reserves the right to disclose information to such bodies or highlight any concern of potential illegal activities being carried out via the Thomson Reuters Managed Services.

3. USE OF MATERIAL

Users remain solely and fully responsible for the content of any material posted, hosted, downloaded, uploaded, created, accessed or transmitted using the Thomson Reuters Managed Services.

Thomson Reuters has no responsibility for any material created or accessible on or through the Thomson Reuters Managed Services that is not posted by or at the request of Thomson Reuters. Thomson Reuters does not monitor nor exercise any editorial control over such material, but reserves the right to do so to the extent permitted by applicable law. Thomson Reuters is not responsible for the content of any websites other than Thomson Reuters' websites, including for the content of websites linked to Thomson Reuters' websites. These links are provided as internet navigation tools only.

4. POLICY VIOLATION

Thomson Reuters is not obliged to take active steps to monitor customer compliance with this Policy. In the event that Thomson Reuters becomes aware of a breach of this Policy, Thomson Reuters may take any or all of the following actions:

- inform a network administrator of an issue or incident;
- require help from a User in resolving a security incident where that User's system(s) may have been involved;
- charge the offending party for the time and resources used in dealing with the breach; or
- in extreme cases with notice suspend or terminate a network connection or connections.

5. REPORTING

Use of the Thomson Reuters Managed Services requires each User to cooperate with Thomson Reuters in responding to security incidents affecting the Thomson Reuters Managed Services and report to Thomson Reuters any event, condition, or activity that provides reasonable suspicion that any of the following have occurred:

- a violation of this Policy; or
- a breach or compromise of the security of the Thomson Reuters Managed Services including, without limitation, any event, condition, or activity occurring within a User's computer network or systems that could affect the security of the Thomson Reuters Managed Services or any computer or network systems of other Users.

6. CONFIDENTIALITY

Users shall hold in confidence any information received from Thomson Reuters, its affiliates and their suppliers and subcontractors related to the security and architecture of the Thomson Reuters Managed Services, including, but not limited to, network routing information, IP addresses, device configurations, topology, host names, system configurations, security access codes, encryption and

authentication keys, passwords, controls, processes, procedures and safeguards. No information of these types may be disclosed for any reason except on a need-to know basis and only to employees, agents, sub-contractors, or other third parties who are contractually bound to non-disclosure obligations.

7. MONITORING

Thomson Reuters reserves the right to monitor all usage of the Thomson Reuters Managed Services for purposes of network management, performance management, capacity planning, and security monitoring and management.

8. OTHER ACTIVITIES

Users must not engage in any activity, either lawful or unlawful, which Thomson Reuters considers detrimental to its subscribers, operations, reputation, goodwill or customer relations.