SS 

Refinitiv Acceptable Use Policy

1. INTRODUCTION

Refinitiv has formulated this acceptable use policy ("Policy") in order to encourage the responsible use of Refinitiv' networks, systems, services, websites and products (collectively "Refinitiv 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 Refinitiv Managed Services
- certain prohibited actions; and
- possible actions by Refinitiv if Users fail to meet those minimum standards.

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

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

Simply exercising good judgment and common sense whilst using the Refinitiv 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 Refinitiv account team.

2. UNACCEPTABLE USE

2.1 Illegal Use. Users are prohibited from using Refinitiv 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. Refinitiv 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 Refinitiv 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 Refinitiv Managed Services is strictly prohibited.

2.4 Unauthorized Access. Refinitiv 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. Refinitiv 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 Refinitiv 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 Refinitiv Managed Services to commit any other form of forgery or illegal or unauthorized impersonation.

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

This prohibition requires that no User use the Refinitiv 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 Refinitiv Managed Services shall occur without the express written consent of Refinitiv.

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

Refinitiv will cooperate with appropriate law enforcement agencies and other parties involved in investigating claims of illegal or inappropriate activity. Refinitiv reserves the right to disclose information to such bodies or highlight any concern of potential illegal activities being carried out via the Refinitiv 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 Refinitiv Managed Services. Refinitiv has no responsibility for any material created or accessible on or through the Refinitiv Managed Services that is not posted by or at the request of Refinitiv. Refinitiv 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. Refinitiv is not responsible for the content of any websites other than Refinitiv' websites, including for the content of websites linked to Refinitiv' websites. These links are provided as internet navigation tools only.

4. POLICY VIOLATION

Refinitiv is not obliged to take active steps to monitor customer compliance with this Policy. In the event that Refinitiv becomes aware of a breach of this Policy, Refinitiv 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 Refinitiv Managed Services requires each User to cooperate with Refinitiv in responding to security incidents affecting the Refinitiv Managed Services and report to Refinitiv 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 Refinitiv 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 Refinitiv Managed Services or any computer or network systems of other Users.

6. CONFIDENTIALITY

Users shall hold in confidence any information received from Refinitiv, its affiliates and their suppliers and subcontractors related to the security and architecture of the Refinitiv 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

Refinitiv reserves the right to monitor all usage of the Refinitiv 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 Refinitiv considers detrimental to its subscribers, operations, reputation, goodwill or customer relations.