VENDOR DATA SECURITY POLICY

Contractor or Vendor, as applicable (hereinafter, each a "Contractor"), agrees that its collection, management and use of CLEAResult Data, as defined in Section 1 below, during the Term shall comply with this Data Security Policy. Capitalized terms not defined in this Data Security Policy are as defined in the Master Services Agreement, Vendor Agreement, License Agreement, Contractor Participation Agreement or other main agreement between CLEAResult and Contractor (the "Master Agreement").

1. CLEAResult Data. CLEAResult Data shall mean:

a. All data or information provided, transferred, uploaded, migrated or otherwise sent to Contractor by or on behalf of CLEAResult, any client of CLEAResult, or any customer of any client of CLEAResult; and

b. Any account number, forecast, or other similar information disclosed to or otherwise made available to Contractor by or on behalf of CLEAResult, any client of CLEAResult, or any customer of any client of CLEAResult.

2. Use and Storage of CLEAResult Data.

a. Contractor may receive CLEAResult Data for the purposes of performing its obligations under the Master Agreement. Subject to the terms of the Master Agreement, CLEAResult grants Contractor a personal, non-exclusive, non-assignable, non-transferable limited license to use the CLEAResult Data solely for the limited purpose of performing its obligations under the Master Agreement during the Term. Contractor shall disclose CLEAResult Data only to its employees with a need to know such information for the performance of the Master Agreement and subject to the terms of this Data Security Policy. Contractor agrees to protect CLEAResult Data with at least the same degree of care used to protect its own most confidential information.

b. Contractor agrees that CLEAResult Data will not be (i) used by Contractor for any purpose other than that of performing Contractor's obligations under the Master Agreement, (ii) disclosed, sold, assigned, leased or otherwise disposed of or made available to third parties by Contractor, (iii) commercially exploited by or on behalf of Contractor, or (iv) provided or made available to any third party without prior written authorization from CLEAResult.

c. Contractor will comply with (i) all applicable international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective relating in any way to the privacy, confidentiality or security of CLEAResult Data ("**Privacy and Data Security Law**"), (ii) all applicable industry standards concerning privacy, data protection, confidentiality or information security, and (iii) all applicable provisions of every Contractor privacy policy, statement, or notice; and (iv) the CLEAResult Privacy Policy, or any similar statement or notice that is provided to Contractor in writing.

d. Contractor shall not store, maintain or process any CLEAResult Data outside the United States of America.

e. Contractor shall not store, maintain or process any CLEAResult Data in any cloud service or facility without the express prior written consent of CLEAResult, which consent may be withheld at the sole discretion of CLEAResult.

3. CLEAResult System Access. Contractor agrees that it may have access to CLEAResult Data on CLEAResult's network, including but not limited to any server, intranet, or other type of information storing and sharing device or conduit owned or operated by CLEAResult (the "CLEAResult Network"), solely for the purpose of meeting its obligations under the Master Agreement. Contractor agrees that access for other purposes, or the use of the CLEAResult Network to access other networks, is strictly forbidden and that Contractor is responsible and liable for all damages or unauthorized access resulting from these actions. Such activity will result in the discontinuation of any and all connections to the CLEAResult Network. Contractor agrees that any use of the CLEAResult Network will be solely for necessary business purposes. In accordance with CLEAResult's existing

network usage policies, Contractor and its employees shall not access any gambling, pornography or hate or violence sites; introduce any viruses, worms, Trojan horses or other bugs or errors in the network; or forward any chain letters, executable "ready to run" files or other files that may cause damage to CLEAResult, its system or the CLEAResult Network. CLEAResult reserves the right to monitor Contractor's use of the CLEAResult Network. Contractor further agrees that any information that it obtains from access to the CLEAResult Network is CLEAResult Data. CLEAResult and Contractor agree that, in the event of a breach or threatened breach of this Section, CLEAResult shall be entitled to specific performance of the provisions of this Data Security Policy and the Master Agreement, including an injunction prohibiting any such breach. Any such relief will be in addition to and not in lieu of any other appropriate relief in the way of money damages or otherwise. CLEAResult reserves the right, in its sole discretion, to terminate Contractor's access to and use of the CLEAResult Network at any time, for any reason, and without notice to Contractor.

4. Security Controls.

a. In addition to any other requirements set forth herein, Contractor will establish and implement appropriate administrative, technical and physical safeguards (i) to ensure the security and confidentiality of CLEAResult Data, (ii) to protect against any anticipated threats to the security or integrity of CLEAResult Data, and (iii) to ensure that CLEAResult Data is not disclosed contrary to the provisions of this Section or any applicable Privacy and Data Security Law.

b. In addition to the specific requirements of this Section, Contractor will develop, implement and maintain a comprehensive data and systems security program ("**Security Program**"). Such Security Program shall include, but shall not be limited to, reasonable and appropriate technical and organizational security measures, procedures and practices against the destruction, loss, unauthorized access or alteration of CLEAResult Data, including but not limited to:

i. Written policies regarding information security, disaster recovery, third-party assurance auditing, penetration testing;

ii. Password protected workstations at Contractor's premises, any premises where the Contractor is performing its obligations under the Master Agreement, and any premises of any third party who has access to CLEAResult Data;

iii. Encryption of Confidential Information, as defined in the Master Agreement, including but not limited to any personally identifiable information of clients of CLEAResult or, or any customer of any client of CLEAResult.

iv. Measures to safeguard against the unauthorized access, destruction, use, alteration or disclosure of any CLEAResult Data including, but not limited to, restriction of physical access to CLEAResult Data, implementation of logical access controls, sanitization or destruction of media, including hard drives, and establishment of an information security program that at all times is in compliance with the current standard requirements in the industry.

c. CLEAResult shall have the right to monitor Contractor's compliance with the terms of this Section. During normal business hours and with twenty-four (24) hours prior notice, CLEAResult or its authorized representatives may inspect Contractor's facilities and equipment and any information or materials in Contractor's possession, custody or control, relating in any way to Contractor's obligations under this Section.

d. In the event, CLEAResult determines Contractor has not complied with this Section, CLEAResult shall provide written notice to Contractor describing the deficiencies. Contractor shall have sixty (60) calendar days from receipt of such notice to cure. If Contractor has not cured the deficiencies within sixty (60) calendar days, CLEAResult may cancel the Master Agreement.

5. Security Maintenance.

a. Prior to CLEAResult's first transfer of CLEAResult Data to Contractor, Contractor shall provide CLEAResult with documentation satisfactory to CLEAResult that it has undertaken an Information Security Program.

b. Contractor shall provide CLEAResult written notice of any material change in its Information Security Program.

c. Contractor and CLEAResult agree to meet upon request of CLEAResult to evaluate the Information Security Program and to discuss, in good faith, means by which the parties can enhance such protection, if necessary.

d. Contractor shall update its Information Security Program, including procedures, practices, policies and controls so as to keep current with applicable industry standards.

6. Security Breach. Contractor shall notify CLEAResult immediately (and, in any case, within twenty-four (24) hours) in writing of any actual, threatened or imminent breach of this Section (regardless of whether there is any identified disclosure, compromise, loss, or damage to CLEAResult Data) or any other unauthorized use, disclosure or acquisition of or access to, or loss of any CLEAResult Data of which Contractor becomes aware. Such notice will summarize in reasonable detail the effect on CLEAResult, if known, of the breach or unauthorized use, disclosure or acquisition of, or access to, or loss of any CLEAResult Data and the corrective action taken or to be taken by Contractor. Contractor will promptly take all necessary corrective actions, and will cooperate fully with CLEAResult in all reasonable and lawful efforts to prevent, mitigate or rectify such breach or unauthorized use, disclosure, acquisition, access or loss, all at Contractor's sole expense, including developing and distributing notices, in writing, to affected persons as required by applicable law, rule, regulation or order or as CLEAResult may otherwise deem necessary or advisable.

7. No Waiver. The failure of either party to enforce strict performance by the other of any provision of this Data Security Policy, or to exercise any right available to that party, shall not be construed as a waiver of such party’s right to enforce strict performance in the same or any other instance.