LeadSquared Information Security Addendum

MarketXpander Services Private Limited ("LeadSquared") and _____ ("Supplier") (each a "Party" and collectively the "Parties") have entered into a master services agreement dated [Contract Execution Date] ("Agreement"). This information security addendum ("Addendum") sets forth the Parties' mutual understanding relating to the privacy and security of LeadSquared Confidential Information and LeadSquared Systems. In the event of any conflict between the terms of this Addendum and the Agreement, the terms of this Addendum would prevail, specifically with respect to information security terms and obligations.

I. CONFIDENTIALITY

1. LeadSquared Confidential Information shall include, without limitation, all (i) information received by Supplier from LeadSquared or collected or generated directly by Supplier on LeadSquared's behalf in connection with the Services, that should reasonably be considered confidential under the circumstances, notwithstanding whether it was identified as such at the time of disclosure; (ii) all information identified as confidential to which Supplier has access in connection with the subject matter of the Agreement, whether before or after the Effective Date of the Agreement; (iii) the Agreement; (iv) all trade secrets; (v) existing or contemplated products, services, designs, technology, processes, technical data, engineering, techniques, methodologies and concepts and any information related thereto; and (vi) information relating to business plans, sales or marketing methods and customer lists or requirements.

2. During the term of the Agreement, Supplier shall take all technical and organizational measures to maintain the security and integrity of any data or Confidential Information made available to it by Customer during the course of rendering the Services. Supplier agrees to comply, with the security related policies, guidelines, standards and requirements as may be notified in writing by LeadSquared from time to time and shall ensure to incorporate such updates by reference. Supplier is deemed to accept all the updates as and when notified by LeadSquared.

3. Supplier shall not: (i) collect, retain, use, access, rent, sell, disclose, reconfigure, de-identify, re-identify or aggregate LeadSquared Confidential Information for any purpose other than to provide the Services as set forth in this Agreement; (ii) retain, use or disclose LeadSquared Confidential Information outside of the direct business relationship between LeadSquared and Supplier; or (iii) use LeadSquared Confidential Information to create any derivative work or product for the benefit of Supplier or any other party without LeadSquared's express, written authorization. Any unauthorized use of LeadSquared Confidential Information shall constitute a material breach of the Agreement and, as a result, LeadSquared may, in its sole discretion, immediately suspend or terminate Supplier's access to LeadSquared Confidential Information and LeadSquared Systems. Supplier certifies that it understands the restrictions set forth in this section and will comply with them.

4. Supplier agrees to establish and maintain, in writing, an information security and privacy policy consistent with this Addendum and applicable laws ("Information Security Policy"). The Information Security Policy shall include appropriate physical, technical and administrative safeguards, including any safeguards and controls agreed by the Parties in writing, sufficient to protect LeadSquared Systems and LeadSquared Confidential Information from unauthorized or unlawful destruction, loss, alteration, disclosure or access. LeadSquared may, at any time pursuant to reasonable notice, review the Information Security Policy and require changes to the same to be line with applicable laws or reasonable technical and industry standards.

5. The Information Security Policy must specifically provide for safeguards for any information identifying, relating to, describing, capable of being associated with or that could be linked, directly or indirectly, with particular persons or households, including but not limited to information derived from such information that is used to create inferences regarding or profiles of such persons or households ("Personal Information"). The Supplier must ensure to establish policies and procedures to and shall implement the mechanisms for encrypting sensitive data in storage, in accordance with applicable laws.

6. Notwithstanding the foregoing, Supplier will be permitted to retain: (i) LeadSquared Confidential Information for a longer period if such retention is strictly necessary to meet Supplier's legal compliance obligations, and (ii) LeadSquared Confidential Information in backup media. Retention of LeadSquared Confidential Information pursuant to (i) and (ii) shall be pursuant to Supplier's fully implemented and documented records management program, provided that such retention shall not be indefinite and shall not exceed industry standards. In addition, LeadSquared Confidential Information so retained shall not be used for any other purpose and such LeadSquared Confidential Information shall be otherwise maintained in accordance with this Addendum.

II. LEADSQUARED SYSTEM

1. Any physical or technical system owned, leased, licensed or operated by LeadSquared or its Affiliates, whether on premises or hosted by a third-party, which processes LeadSquared Confidential Information and is accessed by Supplier in the course of performing the Services, shall constitute a LeadSquared System.

2. Supplier shall ensure that the code written and deployed on any LeadSquared System is safe, secure, and free of any malware or security errors. Supplier shall also ensure that this code shall only perform intended action and desired results.

III. DATA SECURITY

1. During the term of the Agreement, Supplier will comply, at its own cost and expense, with this Addendum, the Information Security Policy, with current and new laws, regulations, governmental requirements, reasonable technical and industry standards relating to Supplier's processing of LeadSquared Confidential Information and any Personal Information. If Supplier is unable to comply with any new law or other requirement under this Addendum, LeadSquared may, in its sole discretion, terminate the Agreement upon notice to the Supplier.

2. Supplier shall define the information security responsibilities of all Supplier employees working in connection to the Services. The Supplier shall ensure that all information security requirements in this Agreement are communicated, including in writing, to all its employees in relation to their role. Furthermore, Supplier's primary information security contact is:

   Name:
   Designation:
   Telephone Number:
   Email Address:

   Supplier agrees to promptly notify LeadSquared of any changes to this information.

3. Supplier shall monitor and, at regular intervals consistent with industry best practices, test and evaluate the effectiveness of its Information Security Policy and Supplier's compliance with the terms of the Agreement. Supplier shall evaluate and promptly adjust its practices with regards to compliance with the Agreement, including its Information Security Policy, in light of the results of the testing and monitoring, any material changes to its operations or business arrangements, or any other facts or circumstances that Supplier knows or reasonably should know may have a material impact on the use or security of LeadSquared Confidential Information and LeadSquared Systems or Supplier's compliance with the terms of the Agreement.

4. Supplier shall ensure that the utility programs capable of potentially overriding system, object, network, virtual machine and application controls shall be restricted.

5. Supplier shall contractually require any and all suppliers, contractors or other agents of Supplier engaged to perform the Services to comply with the terms of this Addendum and all laws. Supplier shall make commercially reasonable efforts to monitor and enforce such contractual requirements and shall be responsible to LeadSquared for all acts or omissions of its subcontractors and agents with respect to their access to and use of LeadSquared Confidential Information and LeadSquared Systems.

6. In case of subcontracting is permitted by LeadSquared, Supplier shall be responsible for all the Services provided to the LeadSquared regardless of which entity is conducting the operations. The Supplier is also responsible for ensuring that the sub-contractor comply with all security/confidentiality requirements and other terms and conditions as applicable to the Supplier mentioned in this Agreement. LeadSquared reserves the right to conduct independent audit in this regard. LeadSquared reserves the right to ask Supplier and Supplier shall change/ amend the clause(s) entered between the Supplier and Subcontractor for LeadSquared's suitability.

7. The Supplier shall be accountable to perform audits at least annually once by the Supplier's internal audit department/corporate governance team/ Supplier appointed third party/ external auditors in order to verify the strength of information security and to validate the compliance with LeadSquared's information security policies and standards. The Supplier shall submit compliance certificate to LeadSquared from an authorized signatory. In addition to this, to monitor Supplier's compliance with the Agreement, LeadSquared may, in its discretion, periodically inspect and audit Supplier's compliance with the Agreement, including its Information Security Policy and any facilities or systems used by Supplier to provide the Services. Such inspections and audits may, at LeadSquared's option, be conducted on-site by LeadSquared personnel or LeadSquared's contracted third party assessors, or through surveys and interviews. Onsite inspections and audits will be conducted during Supplier's ordinary office hours upon reasonable prior written notice by LeadSquared and shall be subject to Supplier's reasonable security restrictions (*e.g.*, sign-in requirements, badge requirements, escort requirements).

IV. CERTIFICATIONS

1. The Information Security Policy shall follow NIST Cybersecurity Framework (CSF), NIST SP:800-53, ISO 27001, SOC2 Type 2, Secure Coding Guidelines and best practices or substantially similar standards applicable to Supplier's industry.

2. Supplier shall maintain a certification or third-party assessment of compliance with the security standards identified in Section 9 of this Addendum provided by a qualified third party reasonably acceptable to LeadSquared. Such certifications shall be provided to LeadSquared upon request.

V. DATA INCIDENT

1. Any breach of Supplier's Information Security Policy leading to the accidental or unlawful or unauthorized destruction, loss, alteration, disclosure of, or access to, LeadSquared Confidential Information shall constitute a data incident as per this Addendum ("Data Incident").

2. Supplier shall promptly notify LeadSquared's Emergency Operations Center within 24 (twenty-four) hours of any Supplier personnel becoming aware of any Data Incident or breach in the Information Security Policy of the Supplier, by a written notice to security@leadsquared.com. The written notice shall summarize, in reasonable detail, the nature and scope of the Data Incident (including a description of all impacted LeadSquared Confidential Information and LeadSquared Systems) and the corrective action already taken or planned by Supplier. The notice shall be timely supplemented to the level of detail reasonably requested by LeadSquared, inclusive of relevant investigative or forensic reports. LeadSquared reserves the right to investigate further and conduct audit/forensic. Such audit/forensic can be done by the LeadSquared's officials or by any other independent auditor. In such an event the auditors may require the chain of custody for collection, retention, and any other information which may be considered as an evidence to support any potential legal action by or against LeadSquared and the Supplier shall ensure to follow standard forensic preservation procedures and instruction of LeadSquared.

3. Supplier shall promptly, at its own cost and expense, take all reasonable and necessary actions to end the Data Incident, mitigate its impact and prevent recurrence. Supplier shall cooperate with LeadSquared in the investigation of the Data Incident and shall promptly respond to LeadSquared's reasonable inquiries about the Data Incident. In the event of a Data Incident, LeadSquared may, in its sole discretion, immediately suspend or terminate Supplier's access to LeadSquared Confidential Information and LeadSquared Systems.

4. Any information pertaining to a Data Incident or Information Security Policy breach shall be kept confidential in perpetuity and Supplier will not inform any third party of a Data Incident, related with LeadSquared without first obtaining LeadSquared's prior written consent, unless and to the extent that Supplier is otherwise required to provide notice by law. The Parties shall collaborate on whether to provide notice of the Data Incident to any person, governmental entity, the media, or other party and the content of any such notice. LeadSquared will make the final determination for LeadSquared related data incident as to whether notice will be provided and to whom, the content of the notice, and which Party will be the signatory to the notice. Supplier shall promptly notify LeadSquared of any investigations of LeadSquared's information use, privacy or information security practices or a Data Incident by a governmental, regulatory or self-regulatory body.

5. Supplier shall ensure to establish policies and procedures and shall implement the mechanisms for vulnerability and patch management. Supplier shall ensure that application, system, and network device vulnerabilities are evaluated and appropriate security patches applied in a timely manner taking a risk-based approach for prioritizing critical patches. In case of any vulnerabilities detected during the security review, Supplier shall close the vulnerabilities within one month without any additional commercials. LeadSquared reserves the right to impose penalties in case of failure to close the 'High' vulnerabilities within one month.

6. Supplier shall provide LeadSquared with prompt written notice if at any time it is not in full compliance with all of the requirements of this Addendum. Supplier shall certify compliance with this Addendum from time to time or as may be reasonably requested by LeadSquared.

VI. DATA TRANSFER

1. LeadSquared Confidential Information may not be transferred, stored, or processed outside the country in which Supplier receives it without prior written approval from LeadSquared, inclusive of transfers to subcontractors or agents. Supplier shall cooperate with LeadSquared in complying with all laws regulating the cross-border transfer of information, and the Parties shall negotiate, in good faith, such additional agreements, terms and conditions as may be required by such laws to effectuate such transfers.

VII. GENERAL

1. RETURN OF INFORMATION: At LeadSquared's direction at any time, and in any event upon termination or expiration of this Agreement, Supplier will immediately cease use of the LeadSquared Confidential Information, including any physical assets that belong to LeadSquared and return the same to LeadSquared and then destroy any and all residual copies of LeadSquared Confidential Information (in whole or part), whether in hard copy or electronic format. Supplier will ensure that LeadSquared Confidential Information is destroyed securely and in accordance with applicable law. As requested, Supplier will certify its compliance with these procedures.

2. INDEMNIFICATION: No limitation of liability provisions, if any, in the Agreement shall apply to any breach of this Addendum by Supplier. Notwithstanding anything in the Agreement to the contrary, Supplier shall indemnify, hold harmless and defend LeadSquared (including its affiliates) from all suits, claims, demands, proceedings and other actions brought by a third party, and pay all direct expenses and costs (including but not limited to, assessments, fines, losses, penalties, settlements, and attorneys' fees, including attorneys' fees incurred in enforcing this indemnification provision), arising out of or related to Supplier's misuse of LeadSquared Confidential Information, any Data Incident or any breach by Supplier of this Addendum.

3. TERMINATION: In addition to any other termination rights under the Agreement, LeadSquared shall have the right to terminate the Agreement immediately if Supplier materially breaches any provision of this Addendum.

4. SEVERABILITY: The invalidity or unenforceability of a portion of this Addendum shall not affect the validity or enforceability of the remainder hereof.