Non-Disclosure Agreement

This One-Way Non-Disclosure Agreement ("Agreement") is entered into and agreed upon by and between you (the "Receiving Party" or "Recipient"), whether an individual or legal entity, and 42Gears Mobility Systems Pvt. Ltd., having its registered office at 1st Floor, 2B, AMR Tech Park, Hosur Main Road, Bommanahalli, Bangalore – 560068, Karnataka, India (hereinafter referred to as the "Disclosing Party" or "Discloser").

1. This Agreement will govern all Confidential Information shared by Disclosing Party to Receiving Party for itself and its subsidiaries and affiliates. For the purposes of this Agreement, the Disclosing Party has agreed to disclose its Confidential Information (as defined hereunder), subject to the terms and conditions contained herein and desires the Receiving Party to treat the said Confidential Information as confidential.

2. **Confidential Information**
   Confidential Information means any non-public information disclosed by the Disclosing Party to the Receiving Party, whether oral, written, electronic, or in any other form, that is not generally known to the public, including, but not limited to information that relates to software, technical/ financial/ marketing/ customer/ business information, specifications, analysis, designs, drawings (including product's workflow and architecture), all or any data shared during the audit process and assessment (including third party audits), pricing, trade secrets, products, services, policies, and procedures, tools, methods, diagrams, prototypes, samples, VAPT Reports ("Vulnerability Assessment and Penetration Testing") (either interim or final), security and audit reports (including third party SOC reports),trade secrets and any other proprietary information that may be disclosed between the parties whether orally or in writing. All information relating to vulnerabilities that you become aware of through the discussions and any other vulnerabilities received by the Receiving Party through any third parties against 42Gears Products and Services is considered confidential ("Confidential Information").
   Confidential Information shall also include any copies, extracts, summaries, or derivations of such information, and all analyses, compilations, studies, or other documents prepared by the Receiving Party that contain or are based on such Confidential Information.

   The Receiving Party acknowledges and confirms the confidential and sensitive nature of all information, documents and material that (i) may be disclosed or made available to the Receiving Party by the Disclosing Party or its employees/ representatives/ advisors/ Consultants (ii) Receiving Party may process or arrive at during the course of the discussion; (iii) Receiving Party may have come across during its discussions with the Disclosing Party; and (iv) All enquiries, negotiations and discussions between the Parties relating to the Vulnerability disclosures and VAPT Reports (all the information referred to above is hereinafter referred to as the "Confidential Information").

VAPT Reports means any or all information derived from the assessment process describing the Disclosing Party's environment, including but not limited to the description of systems, infrastructure, processes, physical conditions, safeguards, vulnerabilities, exposures and remedial measures.

3. **Confidential Obligations**

The Receiving Party shall maintain confidentiality of the Discloser's Confidential Information with reasonable care and discretion and no less than the degree of care used to protect its own Confidential Information to prevent:

a. The Receiving Party shall take reasonable measures to protect Confidential Information shared with respect to the VAPT Reports and shall refrain from sharing it to any third party, contractors, partners, customers or any unauthorized party. No VAPT reports shall be shared with any third party without the consent in writing by the Disclosing Party.
b. The Receiving Party shall make authorized disclosure to only those employees who have similar non-disclosure obligations placed on by the Disclosing Party.
c. The Receiving Party without written authorization shall not publish, reveal, transfer or otherwise disclose the VAPT Reports shared and shall keep such or any information about discovered vulnerabilities confidential in accordance with this Agreement.
d. Any information received or collected about 42Gears through the VAPT reports must be kept confidential and only used in connection with the intended purpose in writing between the Parties.
e. Treat the vulnerability report and any other vulnerabilities received from any third party as Confidential Information and not disclose these VAPT Reports to any third person (except disclosure to 42Gears) any such information until public disclosure is mutually agreed upon with 42Gears.

4. **Exceptions**

Confidential Information shall not include the following:

a. Information known to Recipient prior to it being shared by Discloser;
b. Information available in the public domain without any fault of the Recipient;
c. Information independently developed by the Recipient;
d. Information disclosed by a third party to the Recipient without any confidentiality obligation.

5. **No warranty**

The Confidential Information disclosed hereby is disclosed "as is" without any warranty, responsibility or liability of any manner including that of warranty of fitness for a particular purpose. The Recipient understands and agrees that there is no license or rights granted by 42Gears by any implication, estoppel, or otherwise to Recipient pursuant to this Agreement to use any Confidential Information for any purpose other than for the purpose for disclosure by 42Gears.

6. This Agreement imposes no obligation on the Disclosing Party to share any Confidential Information or get into any contractual arrangement with the Receiving Party.

7. **Ownership**
   All Confidential Information will remain the exclusive property of the Disclosing Party. Recipient will not use any trade name, trademark, logo or any other proprietary rights of the Disclosing Party (or its Affiliates) in any manner without prior authorization of such use by an authorized representative of such Disclosing Party.

8. Recipient acknowledges that breach or threatened breach of any provisions of this Agreement including but not limited to unauthorized and improper disclosure of Confidential Information may cause irreparable damages to the Discloser, therefore Discloser shall be entitled (a) to equitable relief including injunctive relief/temporary restraining order in addition to all other remedies available under law in case of unauthorized and improper disclosure, and (b) to be indemnified by the Receiving Party from any loss or harm, including but not limited to attorney's fees, arising out of or in connection with any breach or enforcement of the Receiving Party's obligations under this Agreement or the unauthorized use or disclosure of the Disclosing Party's Confidential information.

9. **Term and Termination**
   This Agreement will remain in effect for twelve (12) months from the Effective date. Either party may terminate this Agreement by providing a fifteen (15) days' written notice to the other party before the end of the Term. A Receiving Party's obligation to maintain confidentiality will remain in effect for three (3) years from the date of disclosure and will survive termination of the Agreement. Upon termination, or earlier at the request of the Discloser at any time, Recipient will promptly return all Confidential Information and copies, reproductions, summaries, or extracts, thereof to the Discloser. At the Discloser's request, Recipient shall destroy such Confidential Information and certify the same in writing by an authorized signatory of the Recipient.

10. **Audit Right**
    The Disclosing Party reserves the right to audit compliance with this Agreement, including the Receiving Party's data protection practices and internal access logs, upon reasonable notice.

11. **Data Security Commitment**
    The Receiving Party shall implement and maintain appropriate administrative, technical, and physical safeguards to protect the Confidential Information against unauthorized access or disclosure, consistent with industry standards.
    In the event of any suspected or actual data breach, security incident, or unauthorized disclosure involving Confidential Information, the Receiving Party shall immediately (and no later than 24 hours) notify the Disclosing Party, providing full details of the incident and any corrective actions taken.

12. **Governing law and Jurisdiction**
    If the Receiving Party is a:
    a. U.S. or Canadian resident: Laws of the State of Delaware; courts of Delaware have exclusive jurisdiction;
    b. Indian resident: Laws of India; courts in Bengaluru, India, have jurisdiction;
    c. U.K. or EU resident: Laws of England and Wales; courts in England and Wales have exclusive jurisdiction;
    d. Resident of any other country: Laws of India; courts in Bengaluru, India, have jurisdiction. In the event of ambiguity, the laws of India and the courts in Bengaluru shall have fallback jurisdiction.

13. This Agreement does not create any agency or partnership relationship between the parties. This Agreement forms the entire understanding between the parties with respect to Confidential Information and supersedes any prior discussions or understandings between the parties with respect to Confidential Information. This Agreement cannot be assigned or transferred by either party without the prior written consent of the other party. Any modification to this Agreement has to be made in writing between the parties.