AQUARIUS VISION WORKS LLP

Confidentiality Policy

1. Purpose

This Confidentiality Policy outlines the responsibilities of all employees, contractors, and third-party associates in protecting sensitive and confidential information related to Aquarius Vision Works LLP. The policy aims to safeguard proprietary, personal, and confidential information from unauthorized disclosure, ensuring the company's business interests, intellectual property, and privacy rights are protected.

2. Scope

This policy applies to all employees, contractors, consultants, and any third parties who have access to confidential information in any form—whether written, verbal, or electronic—related to Aquarius Vision Works LLP , its clients, partners, and employees.

3. Definitions

- Confidential Information: Any non-public information that is proprietary, sensitive, or could cause harm to the company, its clients, or employees if disclosed. Examples include but are not limited to:
    - Business strategies, plans, and forecasts
    - Client and customer data
    - Intellectual property (designs, patents, trademarks)
    - Financial information
    - Personnel information
    - Trade secrets

- Authorized Disclosure: Sharing of confidential information with individuals or entities who have been granted explicit permission to receive such information for legitimate business purposes.

4. **Obligations of Confidentiality**

All employees, contractors, and associates must:

- Keep confidential information secure and prevent unauthorized access.
- Only use confidential information for authorized purposes related to their job responsibilities.
- Not disclose confidential information to any unauthorized party, either during their employment/contract or after termination.
- Take necessary precautions to ensure that confidential information is not inadvertently disclosed (e.g., locking computers, not discussing confidential matters in public places).

5. Handling of Confidential Information

- **Physical Security:** Documents containing confidential information must be stored in secure locations and only accessed by authorized personnel.
- **Electronic Security:** Confidential information stored electronically must be protected using secure systems, such as encryption, password protection, and network firewalls. Access should be limited based on the principle of least privilege.
- **Third-Party Disclosures:** Any sharing of confidential information with third-party entities (e.g., vendors, contractors) must be governed by a Non-Disclosure Agreement (NDA) or a similar binding contract.

6. Exceptions to Confidentiality

Confidential information may be disclosed in the following limited circumstances:

- When required by law, regulation, or legal process (e.g., a court order or subpoena).
- When explicit, written permission is granted by the owner of the confidential information.
- When necessary to prevent significant harm (e.g., public safety concerns).

7. Reporting Breaches

Any known or suspected breach of confidentiality must be reported immediately to the [Designated Contact Person, e.g., Compliance Officer]. All reports will be investigated, and appropriate corrective actions will be taken.

8. Disciplinary Actions

Failure to comply with this policy may result in disciplinary actions, including but not limited to termination of employment, legal action, or financial penalties, depending on the severity of the breach.

9. Review and Amendments

This policy will be reviewed annually or as required by changes in the law or business operations. Amendments to this policy will be communicated to all relevant parties.

10. Acknowledgment

All employees, contractors, and third parties must acknowledge that they have read, understood, and agree to comply with this policy by signing a confidentiality agreement upon onboarding or contract initiation.