

OpacityVision VR LLC

Mutual Vendor Non-Disclosure Agreement

Mutual confidentiality terms for vendor, reseller, training, implementation, technical, and commercial discussions.

Effective Date	[Insert Effective Date]
OpacityVision VR LLC	Missouri limited liability company
Vendor	[Insert Vendor Legal Name]
Vendor Entity / Address	[Insert Entity Type, State of Formation, and Address]
Website	opacityvision.com
Governing Law	Missouri
Draft Status	Boilerplate (v1.0) — complete bracketed fields and review before use

Complete all bracketed fields and have counsel review this boilerplate before signature or distribution.

1. Agreement and Parties

This Mutual Vendor Non-Disclosure Agreement (this “Agreement”) is entered into as of the Effective Date by and between OpacityVision VR LLC (“Opacity Vision”) and the Vendor identified above (“Vendor”). Opacity Vision and Vendor are each a “Party” and together the “Parties.”

Either Party may disclose Confidential Information as a “Disclosing Party” and may receive Confidential Information as a “Receiving Party.” The obligations in this Agreement apply equally to each Party in those respective roles.

2. Purpose

The Parties may exchange Confidential Information to evaluate, establish, administer, or perform a vendor, reseller, channel-partner, training-provider, enterprise-implementation, platform-access, integration, support, purchasing, or other commercial relationship involving OpacityVision VR LLC (the “Purpose”). The Receiving Party may use Confidential Information only for the Purpose.

3. Confidential Information

“Confidential Information” means nonpublic information disclosed by or on behalf of a Disclosing Party, before or after the Effective Date, in written, oral, visual, electronic, digital, physical, demonstrative, or other form, that is marked confidential or that a reasonable person would understand to be confidential given its nature or the circumstances of disclosure.

Opacity Vision Confidential Information includes, without limitation:

- software, source code, object code, architecture, APIs, integrations, algorithms, databases, cloud infrastructure, credentials, security controls, incident information, logs, vulnerabilities, and technical documentation;
- VR environments, smoke simulations, video assets, file structures, actual-opacity values, answer keys, grading and scoring logic, test-sequence and clip-selection methods, certification safeguards, anti-cheating controls, demonstrations, prototypes, roadmaps, and unreleased features;
- training, lecture, testing, support, implementation, onboarding, operational, research, and quality-control materials and processes;

- pricing, discounts, margins, MAP information, token economics, forecasts, quotes, proposals, contracts, business plans, vendor terms, customer opportunities, customer and prospect lists, and partner strategies; and
- student, administrator, instructor, vendor, facility, certificate, attendance, performance, payment, support, and account records, including personal information and other protected data.

Vendor Confidential Information includes, without limitation, Vendor customer and facility relationships, student or employee rosters, pricing, proposals, contracts, business plans, training methods, proprietary course content, operational processes, technical information, and other nonpublic information supplied for the Purpose.

Confidential Information also includes notes, summaries, extracts, analyses, compilations, models, reports, or other materials prepared by the Receiving Party that contain, reflect, or are derived from Confidential Information.

4. Exclusions

Confidential Information does not include information that the Receiving Party can demonstrate through contemporaneous written records:

- was lawfully known to the Receiving Party without a duty of confidentiality before disclosure by the Disclosing Party;
- becomes publicly available through no breach of this Agreement or other duty by the Receiving Party or its Representatives;
- is received lawfully from a third party that, to the Receiving Party's knowledge, is not prohibited from disclosing it;
- is independently developed by personnel who did not use or access the Disclosing Party's Confidential Information; or
- is approved for release by the Disclosing Party in a signed writing.

A combination of information is not excluded merely because individual elements are public or known unless the combination and its operating principle are also public or known. The Receiving Party bears the burden of establishing an exclusion.

5. Use and Protection Obligations

The Receiving Party will:

- use Confidential Information solely for the Purpose and not for its own unrelated benefit, for the benefit of another person, or to compete with, bypass, disadvantage, or harm the Disclosing Party;
- protect Confidential Information with at least the same degree of care it uses for its own similar confidential information, and no less than reasonable care;
- limit access to Representatives who have a legitimate need to know for the Purpose and who are bound by confidentiality obligations at least as protective as this Agreement;
- not copy, download, record, scrape, extract, decompile, disassemble, reverse engineer, translate, benchmark, train or evaluate an artificial-intelligence system on, or create derivative works from Confidential Information except as expressly authorized in writing or strictly necessary for the Purpose;
- not disclose credentials, answer keys, actual-opacity values, test-integrity controls, student records, security information, or restricted Platform content to unauthorized persons; and
- promptly notify the Disclosing Party after discovering any suspected loss, unauthorized access, use, or disclosure and reasonably cooperate in containment and remediation.

The Receiving Party is responsible for a breach of this Agreement by its Representatives to the same extent as if the Receiving Party committed the breach directly.

6. Representatives

“Representatives” means a Party’s employees, officers, managers, members, contractors, consultants, attorneys, accountants, insurers, financing sources, and service providers who need the information for the Purpose. Disclosure to a prospective investor, acquirer, or financing source is permitted only when reasonably necessary for the Purpose and subject to written confidentiality duties. A Party may not disclose the other Party’s Confidential Information to a competitor of the Disclosing Party without prior written consent.

7. Required Disclosure

If the Receiving Party is required by law, regulation, subpoena, court order, or governmental demand to disclose Confidential Information, it may disclose only the portion legally required. To the extent legally permitted, the Receiving Party will give prompt written notice to the Disclosing Party and reasonably cooperate, at the Disclosing Party’s expense, in seeking a protective order or other confidential treatment. Nothing in this Section limits the protected disclosures described in Section 13.

8. Personal Data, Student Records, and Security Information

Personal information, student and employee records, training and testing results, certificates, authentication information, security data, and incident information must be handled only for the Purpose and in accordance with applicable law and any signed privacy, data-processing, security, or platform terms. If a signed data-processing agreement conflicts with this Agreement regarding the processing of personal data, the data-processing agreement controls for that processing. Confidentiality obligations that provide greater protection remain effective.

9. Ownership; No License or Commitment

All Confidential Information remains the property of the Disclosing Party or its licensors. No patent, copyright, trademark, trade-secret, data, software, publicity, or other intellectual-property right or license is granted by disclosure except the limited right to use Confidential Information for the Purpose. Neither Party is required to disclose information, enter into a transaction, purchase or sell any product or service, or continue discussions. Except as stated in a signed agreement, Confidential Information is provided without warranty as to completeness or accuracy.

10. Return or Destruction

Upon written request or termination of discussions, the Receiving Party will promptly stop using and return or destroy Confidential Information, including copies and derived materials, and will confirm destruction in writing if requested. The Receiving Party may retain one archival copy solely for legal or compliance purposes and may retain routine backup copies that cannot reasonably be isolated, provided retained information remains protected under this Agreement and is not restored or used except for disaster recovery or legal compliance.

11. Term and Survival

This Agreement begins on the Effective Date and continues until terminated by either Party on thirty (30) days’ written notice. Termination does not affect Confidential Information disclosed before termination. The confidentiality and restricted-use obligations continue for five (5) years after each disclosure. Trade secrets remain protected for as long as they qualify as trade secrets under applicable law. Personal data, credentials, answer keys, test-integrity information, and security information remain protected for as long as they remain nonpublic or as otherwise required by law or a signed agreement.

12. Remedies

Unauthorized use or disclosure may cause harm that cannot be adequately remedied by money damages alone. The Disclosing Party may seek temporary, preliminary, and permanent injunctive or other equitable relief, in addition to any other available remedy, without limiting any defenses or requiring waiver of an applicable bond requirement unless permitted by law. Remedies are cumulative and subject to any limitation-of-liability provision in a signed agreement between the Parties that expressly applies to this Agreement.

13. Protected Disclosures and Federal Trade-Secret Notice

Nothing in this Agreement prohibits or restricts either Party or any individual from reporting a suspected violation of law to a federal, state, or local government official or to an attorney; making a disclosure protected by whistleblower law; cooperating with a government investigation; filing a charge or complaint; or receiving a lawful government award. No prior authorization or notice to the other Party is required for such activity.

Notice under 18 U.S.C. § 1833(b): An individual is not criminally or civilly liable under federal or state trade-secret law for disclosing a trade secret in confidence to a federal, state, or local government official, directly or indirectly, or to an attorney, solely to report or investigate a suspected violation of law; or for disclosing a trade secret in a complaint or other document filed under seal in a lawsuit or other proceeding. An individual who brings a retaliation lawsuit for reporting a suspected violation of law may disclose the trade secret to that individual's attorney and use it in the proceeding if any document containing the trade secret is filed under seal and the trade secret is not otherwise disclosed except by court order.

14. Relationship to Other Agreements

This Agreement supplements the Opacity Vision Master Vendor Platform Agreement, Vendor EULA, Privacy Policy, data-processing terms, order forms, reseller terms, and any other signed agreement between the Parties. If a conflict concerns confidentiality or restricted use, the provision affording greater protection to the affected Confidential Information controls unless a later signed writing expressly supersedes this Agreement. A signed data-processing agreement controls as stated in Section 8. This Agreement does not itself create a partnership, agency, employment relationship, exclusivity obligation, non-compete, non-solicitation restriction, reseller right, territory right, or purchase commitment.

15. Governing Law and Venue

If the Parties have signed another agreement containing a governing-law and dispute-venue provision, that provision applies to this Agreement. Otherwise, this Agreement is governed by the laws of Missouri, without regard to conflict-of-law rules, and any action arising from this Agreement must be brought in the state or federal courts located in [Insert Missouri County], Missouri. Each Party consents to personal jurisdiction and venue in those courts.

16. Miscellaneous

This Agreement is the complete agreement between the Parties regarding its subject matter and may be amended or waived only in a writing signed by both Parties. Failure to enforce a provision is not a waiver. If a provision is held unenforceable, it will be modified to the minimum extent necessary, and the remaining provisions remain effective. Neither Party may assign this Agreement without the other Party's prior written consent, except to an affiliate or in connection with a merger, reorganization, change of control, or sale of substantially all relevant assets, provided the assignee assumes this Agreement. Notices must be sent to the notice contacts below and are effective upon confirmed delivery. Headings are for convenience only. This Agreement may be signed in counterparts and by electronic signature, each of which is deemed an original and together constitute one instrument.

17. Signatures

The individuals signing below represent that they are authorized to bind the respective Party. The Effective Date is the date stated above or, if no date is stated, the date of the last signature.

OpacityVision VR LLC	[Insert Vendor Legal Name]
By: _____	By: _____
Name: [Insert Name]	Name: [Insert Name]
Title: [Insert Title]	Title: [Insert Title]
Date: [Insert Date]	Date: [Insert Date]
Notice Email: [Insert Email]	Notice Email: [Insert Email]
Notice Address: [Insert Address]	Notice Address: [Insert Address]