

Platform & Developer Services Agreement

(API, SDK, Enterprise, OEM & White-Label Terms)

Vizbl Systems, Inc.

Effective Date: August 4, 2026 | Last Updated: August 4, 2026

This Platform & Developer Services Agreement (“Developer Agreement”) is entered into by and between Vizbl Systems, Inc., a Delaware corporation (“Vizbl”), and the customer, developer, or other entity identified in an applicable Order Form or that accepts this Developer Agreement (“Customer”). It governs Customer’s use of Vizbl APIs, SDKs, developer tools, enterprise integrations, OEM deployments, and white-label services.

This Developer Agreement applies only together with an applicable Vizbl Master Services Agreement (“MSA”) or Order Form accepted by Customer. If Customer has accepted or executed an MSA, this Developer Agreement forms part of that MSA. If Customer has not accepted an MSA, the Vizbl Terms of Use govern Customer’s access until Customer accepts an MSA or Order Form that expressly incorporates this Developer Agreement. Capitalized terms not defined here have the meanings given in the applicable MSA or, if no MSA applies, the Terms of Use.

By signing an Order Form, electronically accepting this Developer Agreement, accessing Developer Tools, or deploying a Customer Application using the Developer Services, Customer agrees to be bound by this Developer Agreement.

1. Definitions

“**API**” means any application programming interface, endpoint, webhook, authentication mechanism, or related interface made available by Vizbl.

“**Customer Application**” means a website, mobile application, software product, device, service, or system owned or controlled by Customer into which Developer Tools or Developer Services are integrated.

“**Customer Content**” means all data, catalogs, product information, images, photographs, video, prompts, 3D models, CAD files, textures, materials, trademarks, logos, personal data, and other materials submitted or made available by or for Customer.

“**Developer Documentation**” means Vizbl’s then-current API, SDK, implementation, security, versioning, integration, and usage documentation.

“**Developer Services**” means Vizbl APIs, SDKs, web viewers, hosted viewers, embeds, plugins, webhooks, App Clips, mobile experiences, developer dashboard, enterprise integrations, OEM or white-label deployments, and related support and services.

“**Developer Tools**” means SDK binaries, object code, sample code, libraries, API clients, plugins, embed code, documentation, credentials, keys, tokens, and related technical materials supplied by Vizbl.

“**End User**” means a person who accesses or interacts with a Customer Application or Vizbl-powered experience made available by Customer.

“Generated Output” means any image, text, 3D model, material, texture, segmentation, classification, placement, render, visualization, recommendation, conversion, or other output produced or modified through automated, AI, machine-learning, computer-vision, AR, or 3D functionality.

“OEM Deployment” means a deployment in which Developer Services are embedded in Customer hardware, software, or services for Customer’s own business use or distribution, as expressly authorized in an Order Form.

“Production Use” means use of Developer Services in a live Customer Application made available to End Users.

“White-Label Deployment” means an authorized deployment in which Customer branding replaces or obscures specified Vizbl branding as described in an Order Form.

2. Scope; Relationship to Other Agreements

2.1 Scope. This Developer Agreement applies only to Developer Services expressly ordered, enabled, or used by Customer. No feature, version, capacity, support level, white-label right, OEM right, redistribution right, or service level applies unless included in an Order Form or enabled plan.

2.2 MSA. The MSA governs general commercial, confidentiality, payment, warranty, indemnification, liability, suspension, termination, and dispute-resolution matters. This Developer Agreement adds service-specific terms for Developer Services.

2.3 DPA and SLA. The Vizbl Data Processing Addendum applies where Vizbl Processes Customer Personal Data as a Processor or Service Provider. The Vizbl Service Level Agreement applies only when expressly incorporated into an Order Form and only to the Covered Services identified there.

2.4 Order of Precedence. In the event of conflict: (a) an Order Form controls only if it expressly identifies the provision it overrides; (b) the MSA controls general commercial and legal matters; (c) the DPA controls Processing of Customer Personal Data; (d) the SLA controls availability commitments and service credits; (e) this Developer Agreement controls Developer Services; (f) an applicable SOW controls only the professional-service deliverables it specifically describes; and (g) Documentation and Policies follow.

3. License Grant and Authorized Use

3.1 Development License. During the applicable Subscription Term, Vizbl grants Customer a limited, non-exclusive, non-transferable, non-sublicensable right to access and use the Developer Services solely to develop, test, operate, and support Customer Applications for Customer’s internal business purposes and authorized End-User experiences. This license may be suspended or terminated only in accordance with this Developer Agreement, the MSA, and the applicable Order Form.

3.2 Production Distribution. Where an Order Form authorizes Production Use, Customer may reproduce and distribute the applicable SDK object code solely as inseparably embedded in the Customer Applications, package names, bundle identifiers, domains, app-store accounts, brands, legal entities, and distribution channels identified in the applicable Order Form or registered with Vizbl. Customer may not distribute source code, standalone SDK components, credentials, documentation, sample code, or Developer Tools in a form that enables independent reuse. Any material change to the

ownership, operator, bundle identifier, package name, domain, brand, legal entity, or distribution model of a Customer Application requires Vizbl's prior written approval.

3.3 Affiliates and Contractors. Customer may permit its Affiliates and contractors to exercise Customer's rights solely on Customer's behalf, subject to written obligations at least as protective as this Developer Agreement. Customer remains fully responsible for their acts and omissions.

3.4 No Implied Rights. All rights not expressly granted are reserved by Vizbl and its licensors. No license is granted by implication, estoppel, exhaustion, or otherwise.

4. SDK and API Distribution Restrictions

Customer will not, and will not permit any Affiliate, contractor, End User, or third party to:

- Distribute, sublicense, sell, lease, rent, timeshare, publish, or make Developer Tools available as standalone products or services.
- Expose Developer Services through a general-purpose API, SDK, platform, service bureau, reseller service, or infrastructure service for third parties, except as expressly authorized in an Order Form.
- Enable extraction, replacement, repackaging, re-signing, or reuse of SDK components outside the authorized Customer Application.
- Share API keys, secrets, tokens, private certificates, account credentials, or non-public Documentation with unauthorized persons.
- Use one Customer account, license, key, or quota across unrelated legal entities, applications, brands, or deployments unless expressly permitted.
- Remove copyright, trademark, attribution, telemetry, license, or proprietary notices except as expressly allowed for an authorized White-Label Deployment.

5. Customer Applications and End Users

5.1 Customer Responsibility. Customer is solely responsible for Customer Applications, including design, code, security, hosting, content, data flows, product claims, commerce, payments, accessibility, testing, support, maintenance, and compliance with law and third-party platform rules.

5.2 End-User Terms and Notices. Customer must provide End Users with legally sufficient terms, privacy notices, permissions, disclosures, and consent mechanisms covering Customer Applications and any camera, photo, sensor, location, analytics, or personal-data processing.

5.3 App Stores. Customer is responsible for Apple App Store, Google Play, marketplace, device, carrier, and platform compliance, submissions, fees, review decisions, disclosures, age ratings, privacy labels, data-safety forms, and updates. Vizbl does not guarantee approval or continued distribution.

5.4 Vizbl Technical Disclosures. Vizbl will make available then-current technical information reasonably necessary for Customer to complete applicable app-store privacy, security, and data-practice disclosures regarding the Developer Services in Vizbl's standard configuration. Customer remains solely responsible for the accuracy and completeness of its final disclosures because they depend on Customer's configuration, code, data flows, and use of third-party services.

5.5 Support Allocation. Unless an Order Form states otherwise, Customer provides first-line support to

End Users. Vizbl provides support to Customer through Vizbl's designated support channels, not directly to End Users.

6. Credentials, Security, and Technical Controls

6.1 Credential Protection. Customer must protect all credentials using industry-standard safeguards, least-privilege access, secure secret storage, rotation, and prompt revocation. Credentials may not be embedded in publicly accessible client code unless specifically designed by Vizbl for that purpose.

6.2 Security Incidents. Customer must notify security@vizbl.com without undue delay after becoming aware of unauthorized access, credential compromise, misuse, or a security event involving Developer Services or Vizbl data, and must reasonably cooperate in containment and remediation.

6.3 Testing Restrictions. Customer may not perform penetration testing, vulnerability scanning, load testing, denial-of-service testing, or security research against Vizbl systems without Vizbl's prior written authorization and agreed scope.

6.4 Protective Measures. Vizbl may revoke credentials, require updates, block traffic, isolate an integration, or suspend access where reasonably necessary to protect security, privacy, service integrity, legal compliance, or third parties.

7. Usage Limits, Metering, and Infrastructure Protection

7.1 Limits. Customer must comply with applicable rate limits, concurrency limits, file-size limits, storage limits, bandwidth limits, generation limits, quotas, geographic restrictions, supported environments, and fair-use controls.

7.2 Metering. Vizbl's logs and metering records control usage calculations absent manifest error. Retries, failed requests, generated assets, data transfer, storage, rendering, API calls, active objects, End-User sessions, and other measured events may be billable as stated in the Order Form or plan.

7.3 Abuse. Customer may not circumvent limits, distribute traffic to evade quotas, create duplicate accounts, cache content contrary to Documentation, scrape services, automate unauthorized requests, or use Developer Services in a manner that threatens system stability.

8. Versioning, Updates, Deprecation, and Compatibility

8.1 Changes. Vizbl may update, replace, version, or modify APIs, SDKs, models, endpoints, schemas, authentication methods, features, operating requirements, and Documentation.

8.2 Deprecation. Vizbl may deprecate or discontinue versions. Where commercially reasonable for a generally available paid production interface, Vizbl will use reasonable efforts to provide advance notice or migration information. Immediate changes may occur for security, legal, safety, third-party, or critical operational reasons.

8.3 Supported Versions. Customer must use supported versions and implement required updates within the period specified by Vizbl. Vizbl has no obligation to support deprecated, modified, forked, unsupported, or non-compliant versions.

8.4 Mandatory Security and Compatibility Updates. Customer must implement any update designated

by Vizbl as security-critical, legally required, or necessary for continued compatibility within the period specified by Vizbl. Vizbl may disable unsupported or non-compliant versions after that period and may act sooner where reasonably necessary to address an urgent security, legal, safety, or service-integrity risk.

8.4 No Backward-Compatibility Warranty. Vizbl does not warrant perpetual backward compatibility, identical output, uninterrupted third-party compatibility, or continued availability of any specific model, feature, endpoint, SDK version, device, browser, or operating system.

9. Intellectual Property and Feedback

9.1 Vizbl Property. Vizbl and its licensors retain all right, title, and interest in the Platform, Developer Services, Developer Tools, source code, object code, APIs, SDKs, viewers, rendering systems, AI models, computer-vision systems, workflows, schemas, Documentation, designs, trademarks, telemetry, improvements, and derivative works.

9.2 Customer Content. Customer retains ownership of Customer Content. Customer grants Vizbl and its service providers a non-exclusive, worldwide, royalty-free license during the applicable term and permitted retention period to host, store, reproduce, transmit, cache, convert, optimize, adapt, render, display, analyze, and otherwise process Customer Content as necessary to provide, secure, maintain, support, and operate the Services and comply with law.

9.3 Service Improvement. Vizbl may use Service Data and aggregated or de-identified information that does not identify Customer, an individual, or Customer's confidential assets and is not reasonably capable of re-identification for analytics, security, benchmarking, capacity planning, and service improvement.

9.4 Feedback. Customer grants Vizbl a perpetual, irrevocable, worldwide, transferable, sublicensable, royalty-free right to use and exploit Feedback without restriction or compensation, provided Vizbl does not publicly identify Customer as the source without permission.

10. AI, Generated Outputs, AR, and Computer Vision

10.1 Probabilistic Results. AI, generative-AI, machine-learning, computer-vision, AR, 3D, tracking, segmentation, placement, sizing, surface detection, fitment, and rendering functions are probabilistic and may produce inaccurate, incomplete, inconsistent, delayed, biased, non-unique, offensive, or infringing results.

10.2 Human Review. Customer is solely responsible for reviewing, testing, validating, moderating, approving, and clearing rights in Generated Outputs before publication, advertising, sale, manufacturing, installation, distribution, or reliance.

10.3 No Professional Reliance. Generated Outputs and visualizations are not engineering, architectural, construction, manufacturing, medical, legal, safety, fitment, regulatory, or professional advice. Customer must independently verify dimensions, scale, colors, materials, fit, compatibility, clearances, installation requirements, and compliance.

10.4 Output Use and Ownership Limits. Subject to Customer's compliance with this Developer Agreement and payment of all applicable fees, Customer may use Generated Outputs created for Customer for its business purposes. Vizbl does not assign or transfer ownership of any underlying model,

algorithm, workflow, template, software, library, tool, or technology used to create Generated Outputs. Vizbl does not represent or warrant that any Generated Output is unique, non-infringing, or eligible for copyright, patent, trademark, or other intellectual-property protection.

10.4 Training Restriction. Unless Customer expressly authorizes otherwise in writing, Vizbl will not use Customer Content or Customer Personal Data to train general-purpose or shared AI models for the benefit of other customers or third parties. This restriction does not prohibit processing needed to provide Customer-specific functionality or use of properly aggregated or de-identified Service Data as permitted above.

10.5 Camera-Based Features. Unless expressly stated otherwise, camera-based and try-on features are intended for visualization and placement, not to identify an individual or create an identity profile. Customer is responsible for legally required notices and consents.

11. Customer Content, Rights, and Compliance

11.1 Rights. Customer represents and warrants that it has all rights, permissions, licenses, consents, lawful bases, and authority necessary for Vizbl to process Customer Content and provide the Developer Services.

11.2 Responsibility. Customer is solely responsible for the legality, accuracy, completeness, quality, safety, product claims, dimensions, labeling, accessibility, regulatory status, and non-infringement of Customer Content and Customer Applications.

11.3 Restricted Data. Customer must not submit government identification numbers, payment-card data, protected health information, precise biometric identifiers, children's data, or other highly sensitive or regulated data unless expressly authorized in an Order Form and supported by appropriate contractual and technical controls.

11.4 Takedown. Vizbl may remove, block, disable, or restrict Customer Content or functionality in response to credible infringement claims, legal demands, app-store requirements, safety concerns, policy violations, or material risk.

12. Privacy and Data Protection

12.1 Roles. Customer is responsible for determining whether and how Customer Applications collect or process personal data, for providing notices and obtaining consents, and for configuring Developer Services consistently with applicable Data Protection Laws.

12.2 DPA. Where Vizbl Processes Customer Personal Data on Customer's behalf, the then-current Vizbl Data Processing Addendum is incorporated into and forms part of the applicable agreement.

12.3 Data Disclosures. Customer must accurately disclose data practices required by app stores, regulators, and End-User notices, including data collected or processed through Vizbl SDKs or APIs. Customer must not represent that Vizbl independently controls Customer's End-User relationship unless applicable law requires otherwise.

12.4 Children. Customer may not knowingly use Developer Services in an application directed to children or process children's personal data without Vizbl's prior written approval and legally sufficient parental-consent and compliance mechanisms.

13. Third-Party Services and Open-Source Components

13.1 Third Parties. Developer Services may depend on cloud providers, operating systems, app stores, browsers, devices, AI providers, CDNs, ecommerce platforms, payment providers, and other Third-Party Services. Vizbl is not responsible for their availability, changes, policies, approvals, data practices, or failures.

13.2 Open Source. Developer Tools may include open-source or third-party components governed by separate license terms. Those license terms control solely for the applicable component. Customer must preserve required notices and comply with applicable licenses.

13.3 Customer Integrations. Customer is responsible for third-party integrations selected or configured by Customer, including credentials, permissions, data mapping, security, costs, and compliance.

14. White-Label and OEM Deployments

14.1 Authorization Required. White-Label Deployments and OEM Deployments are permitted only when expressly identified in an Order Form. No white-label, private-label, OEM, resale, or redistribution right arises from ordinary use of Developer Services.

14.2 Branding. The Order Form will specify permitted branding changes and any required “Powered by Vizbl” or other attribution. Customer may not misrepresent ownership of Vizbl technology or remove legal, privacy, security, or required attribution notices.

14.3 No Core Technology Transfer. Customer receives no ownership of, or right to expose, license, or commercialize, Vizbl’s underlying platform, infrastructure, APIs, SDKs, models, source code, hosting, or proprietary technology as Customer’s own platform.

14.4 End-Customer Responsibility. If authorized to provide a Vizbl-powered deployment to Customer’s business clients, Customer remains responsible for those clients, their End Users, contractual flow-down terms, support, billing, privacy compliance, and use of the Services.

15. Competitive and Technical Restrictions

Customer will not, and will not permit any Affiliate, contractor, End User, or third party to:

- Reverse engineer, decompile, disassemble, decode, translate, modify, or attempt to derive source code, algorithms, model weights, training data, non-public schemas, architecture, or proprietary methods, except to the limited extent such restriction is prohibited by law.
- Benchmark or publish performance, security, or comparative testing results without Vizbl’s prior written consent.
- Copy, replicate, emulate, frame, mirror, or create derivative products from Vizbl user interfaces, workflows, Developer Tools, or non-public functionality.
- Use Developer Services, Outputs, Documentation, or access to train, develop, improve, validate, or commercialize a competing AR, 3D, visualization, AI, asset-generation, viewer, SDK, API, or platform service.
- Circumvent security, authentication, metering, watermarks, attribution, rate limits, geographic controls, billing mechanisms, or technical restrictions.

- Use Developer Services for unlawful surveillance, deceptive impersonation, non-consensual intimate imagery, child sexual abuse material, weapons targeting, illegal discrimination, fraud, or other prohibited uses.

16. Fees, Payment, Taxes, and Commercial Terms

16.1 Order Form. Fees, Subscription Term, usage allowances, overages, implementation fees, minimum commitments, support, white-label fees, OEM fees, and payment terms are stated in the Order Form or applicable plan.

16.2 Changes. Vizbl may change pricing and packaging for future purchases or renewal terms. Changes during a committed paid term apply only as permitted by the MSA or Order Form, including changes caused by Customer usage, taxes, law, or pass-through third-party costs.

16.3 Suspension for Nonpayment. Vizbl may suspend Developer Services for overdue amounts in accordance with the MSA. Customer remains liable for fees incurred before and during a suspension caused by Customer.

16.4 No Setoff. Except as expressly permitted in the MSA or required by law, Customer may not withhold, offset, or deduct amounts based on alleged claims or credits.

17. Support, Availability, and Maintenance

17.1 Standard Support. Unless otherwise stated in an Order Form, Vizbl provides standard support during normal business hours through designated support channels. Support response times are targets, not resolution guarantees.

17.2 SLA. No uptime, service-credit, response-time, or availability commitment applies unless the Order Form expressly incorporates the Vizbl Service Level Agreement. Service credits under the SLA are the sole and exclusive remedy for qualifying availability failures.

17.3 Maintenance. Vizbl may perform scheduled and emergency maintenance, deploy security patches, rotate credentials, and make changes required for law, safety, third-party compatibility, performance, or service integrity.

18. Monitoring, Compliance Verification, and Audit

18.1 Monitoring. Vizbl may monitor usage, logs, traffic, errors, security events, integration configuration, and technical metadata to operate, secure, meter, support, and enforce the Services.

18.2 Verification. Upon reasonable request, Customer will provide information reasonably necessary to verify compliance, including application identifiers, package names, domains, deployment scope, distribution channels, End-User volume, and use of credentials.

18.3 Audit Limits. Any audit will be limited to records relevant to Developer Services, conducted during normal business hours on reasonable notice, subject to confidentiality and security restrictions, and may not expose other customers' information or Vizbl source code, vulnerability data, or trade secrets.

18.4 Frequency and Alternatives. Vizbl may conduct no more than one routine compliance audit in any twelve-month period, except where Vizbl reasonably suspects misuse, credential sharing, security risk,

material underreporting, infringement, or breach. Vizbl may first use questionnaires, certifications, logs, and remote review instead of an on-site audit.

18.5 Audit Costs and Underreporting. Each party bears its own routine audit costs. Customer will reimburse Vizbl's reasonable audit costs if an audit identifies a usage underpayment exceeding five percent (5%) for the reviewed period or a material breach. Customer must promptly pay all underreported fees, taxes, and applicable charges, without limiting Vizbl's other rights or remedies.

19. Suspension and Termination

19.1 Suspension. Vizbl may immediately suspend, throttle, revoke credentials, or restrict Developer Services where reasonably necessary for security, abuse, legal compliance, nonpayment, policy violations, app-store or third-party requirements, excessive usage, or risk to Vizbl, customers, End Users, or third parties.

19.2 Termination. This Developer Agreement remains effective for the applicable Subscription Term and terminates with the governing MSA or applicable Order Form, unless earlier terminated under those documents.

19.3 Effect. Upon termination, Customer must cease new use, remove Developer Tools from future distributions, disable credentials as directed, and stop representing that it is authorized to use Developer Services. Vizbl may immediately disable access for security, abuse, infringement, nonpayment, legal, or material-breach reasons. For ordinary expiration or non-renewal, unless the Order Form states otherwise, Customer may receive up to thirty (30) days to remove Developer Tools from already distributed Customer Applications, provided Customer pays all applicable wind-down fees, complies with this Developer Agreement, and does not initiate new End-User deployments. Access ends automatically when the wind-down period expires.

19.4 Survival. Payment obligations, usage restrictions, confidentiality, intellectual property, disclaimers, indemnification, liability limitations, dispute resolution, and provisions that by their nature should survive will survive termination.

20. Warranties and Disclaimers

20.1 Limited Performance Warranty. Any express warranty applicable to paid Developer Services is stated solely in the MSA or Order Form.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, DEVELOPER SERVICES, DEVELOPER TOOLS, DOCUMENTATION, GENERATED OUTPUTS, BETA FEATURES, THIRD-PARTY SERVICES, AND ALL RELATED MATERIALS ARE PROVIDED "AS IS" AND "AS AVAILABLE." VIZBL DISCLAIMS ALL IMPLIED, STATUTORY, AND OTHER WARRANTIES, INCLUDING MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, ACCURACY, SECURITY, AVAILABILITY, COMPATIBILITY, AND RESULTS.

VIZBL DOES NOT WARRANT APP-STORE APPROVAL, BACKWARD COMPATIBILITY, UNINTERRUPTED OPERATION, ERROR-FREE CODE, EXACT VISUALIZATION, SCALE, FIT, COLOR, TRACKING, PLACEMENT, OR ANY PARTICULAR BUSINESS, SALES, CONVERSION, OR PERFORMANCE RESULT.

21. Indemnification and Limitation of Liability

21.1 Governing Terms. Indemnification obligations and limitations of liability are governed by the MSA. This Developer Agreement does not create a separate or additional liability cap.

21.2 Customer Claims. Without limiting the MSA, Customer's indemnification obligations include claims arising from Customer Applications, End-User notices or consent, Customer Content, app-store submissions, product claims, privacy or biometric claims, Customer's distribution or use of Developer Tools, and Customer's breach of this Developer Agreement.

21.3 Service Credits. Any approved SLA credit counts toward and does not increase any aggregate limitation of liability under the MSA.

22. Confidentiality

22.1 MSA or NDA. Confidential Information is protected under the MSA and any applicable NDA. Developer Tools, non-public Documentation, credentials, pricing, roadmaps, security information, architecture, source code, and technical materials are Vizbl Confidential Information.

22.2 Publicity. Neither party may publicly disclose the other party's non-public integration details without permission, except that approved customer-reference and portfolio rights may be stated in an Order Form or MSA.

23. Compliance with Laws; Export and Sanctions

23.1 General Compliance. Customer will comply with applicable privacy, consumer-protection, advertising, accessibility, intellectual-property, export-control, sanctions, anti-bribery, app-store, telecommunications, and product laws.

23.2 Export. Customer may not access, export, re-export, transfer, or use Developer Services in violation of U.S. export controls or sanctions or for prohibited military, weapons, surveillance, nuclear, chemical, biological, missile, or other restricted end uses.

23.3 Restricted Parties. Customer represents that it is not a prohibited or restricted party and is not located in, organized under the laws of, or ordinarily resident in a comprehensively sanctioned jurisdiction, except as authorized by applicable law and Vizbl in writing.

24. General Provisions

24.1 Changes. Vizbl may update this Developer Agreement for future orders and renewals. Materially adverse changes will not apply during a committed paid term unless required for law, security, safety, third-party services, or urgent operational reasons.

24.2 Assignment. Assignment is governed by the MSA. Customer may not transfer credentials, licenses, or deployment rights through a change of control or asset transfer unless the governing agreement permits assignment.

24.3 Entire Agreement. This Developer Agreement, the MSA, Order Forms, DPA, SLA, SOWs, applicable Policies, and expressly incorporated documents constitute the agreement governing Developer Services and supersede prior developer terms on the same subject.

24.4 Electronic Acceptance. Electronic signatures, click-through acceptance, and electronic records are binding to the extent permitted by law.

24.5 Governing Law and Disputes. Governing law, arbitration, venue, jury-trial waiver, and class-action waiver are governed by the MSA. If no MSA applies, dispute resolution is governed by the Vizbl Terms of Use. Nothing prevents either party from seeking temporary or injunctive relief for intellectual-property, confidentiality, security, or unauthorized-access matters where permitted by the governing agreement.

25. Contact Information

Vizbl Systems, Inc.

155 S. Fair Oaks Ave, Suite 1005

Pasadena, California 91105, United States

Legal: legal@vizbl.com

Security: security@vizbl.com

Support: support@vizbl.com

Schedule 1 - Developer Service Categories

This Schedule describes categories that Vizbl may offer from time to time. It does not represent that every feature is generally available, production-ready, included in a plan, available in every jurisdiction, or supported for every Customer. Only Services expressly included in an Order Form, enabled account, or applicable plan are licensed.

Category	Examples
APIs and Webhooks	REST APIs, authentication, asset and catalog endpoints, generation endpoints, configuration endpoints, analytics endpoints, webhooks, callbacks, and related interfaces.
Mobile SDKs	iOS SDK, Android SDK, AR placement, rendering, object interaction, product selection, materials, variants, tracking, camera and sensor integration, and related components.
Web and Embedded Tools	Web AR Viewer, 3D Viewer, AR + 3D Viewer, Room Viewer, embeds, plugins, hosted pages, share links, QR experiences, and web components.
Core AR & 3D	Standard AR, One-Click AR, Multi-Item AR / Multi-AR, smart placement, configurators, product variants, materials, colors, finishes, modules, screenshots, and analytics.
Specialty Visualization	AR Rugs, AR Flooring, AR Wall Art, Showroom AR, Construction AR, AutoFit AI, Virtual Try-On, and related supported workflows.
AI and Automated Services	Photo-to-3D, AI model generation, image generation and editing, home staging, scene generation, segmentation, detection, classification, materials, textures, and recommendations.
Mobile Distribution	iOS App Clips, Android experiences, native applications, QR codes, hosted share pages, and supported mobile distribution channels.
Ecommerce and Platform Integrations	Shopify, WooCommerce, WordPress, Wix, BigCommerce, Squarespace, Webflow, custom storefronts, CRM, POS, catalog, and inventory integrations where supported.

Enterprise Deployments	Branded applications, customer portals, private catalogs, offline or cached catalogs, device deployments, implementation, custom configuration, and managed integrations.
White-Label and OEM	Authorized rebranding, embedded deployment in Customer products, approved distribution to Customer business clients, and related enterprise rights stated in an Order Form.
3D and Digital Asset Services	3D modeling, CAD conversion, optimization, compression, retopology, texturing, materials, rendering, animation, and conversion among supported formats such as GLB, glTF, USDZ, FBX, and OBJ.

Schedule 2 - Responsibility Matrix

Area	Vizbl Responsibility	Customer Responsibility
SDK/API functionality	Provide enabled Developer Services substantially as described in Documentation and applicable Order Form.	Integrate, configure, test, deploy, monitor, and maintain Customer Applications.
Customer interface and commerce	Provide Vizbl components included in the ordered Services.	Navigation, catalog UI, checkout, payments, pricing, product claims, accessibility, and business logic.
Credentials and security	Issue credentials and operate Vizbl-controlled security controls.	Secure credentials, devices, applications, environments, and user access; notify incidents.
End-User privacy	Process data as described in the DPA and Privacy Policy.	Provide notices, obtain consent, configure collection, respond to End Users, and complete app-store disclosures.
App-store distribution	Provide reasonable technical information about Vizbl components.	Developer accounts, submissions, review, fees, ratings, privacy labels, policy compliance, and updates.
Content and product accuracy	Process Customer Content through ordered Services.	Rights, legality, dimensions, specifications, claims, safety, product fit, and approval of outputs.
Support	Provide Customer support at the purchased level.	Provide first-line End-User support and complete diagnostic information.
Third-party systems	Maintain Vizbl-selected providers as commercially reasonable.	Maintain Customer-selected systems, accounts, integrations, permissions, and fees.

Schedule 3 - White-Label / OEM Order Form Checklist

The following items should be completed in the applicable Order Form when Customer receives White-Label or OEM rights:

- Authorized Customer Application names, bundle identifiers, package names, domains, brands, and legal entities.
- Permitted distribution channels, territories, customer groups, devices, and number of deployments.
- Permitted branding changes and required Vizbl attribution or legal notices.
- Whether Customer may distribute to its own business clients and required contractual flow-down

terms.

- Usage commitments, active-object limits, API quotas, storage, bandwidth, generation limits, and overage pricing.
- Support allocation, escalation contacts, maintenance responsibilities, and applicable SLA.
- Data roles, subprocessors, data locations, DPA applicability, and End-User notice obligations.
- App-store account ownership, signing certificates, device-management responsibilities, and release control.
- Exit assistance, wind-down period, data export, credential revocation, and post-termination treatment.
- Any limited exclusivity, custom development, source-code escrow, or ownership term, which applies only if expressly written and signed by Vizbl.

Accepted and Agreed

VIZBL SYSTEMS, INC.	CUSTOMER
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____
Order Form / Account: _____	Legal Name: _____