Master Subscription Agreement

Last Updated: *June 24, 2025*

This Master Subscription Agreement ("**Agreement**") is entered into by and between InfoVision, Inc. ("**InfoVision**" or "**Service Provider**"), the owner of the online platform AlphaMetricx (the "**Platform**"), and the entity that has executed this Agreement by signing an Order Form or availing itself of the Services that incorporate or reference this Agreement ("**Customer**" or "**You**"). Capitalized terms not otherwise defined herein shall have the meanings ascribed to them in the Definitions section below. This Agreement governs the terms and conditions applicable to the Services and any Order Forms executed pursuant to this Agreement.

Definitions.

"**Author Data**" refers to any written, audio, video, or multimedia content published or contributed on publicly accessible platforms or social media networks (including but not limited to Twitter, Instagram, Facebook, LinkedIn, and Reddit) by journalists, bloggers, social media influencers, researchers, analysts, public speakers, or any other individuals ("**Content Authors**"), which is collected and processed by the Platform.

"**Customer Data**", "**Personal Information**" means all data (including Personal Data). Text, images, audio, video, photographs, and other content and material, in any format, provided by Customer or any of Customer's Users that is stored in, or run on or through, the platform by using Services.

"**Deliverables**" means anything developed by InfoVision, including training materials, and delivered to Customer as part of the Professional Services.

"**Order Form**" means an order form as attached as Exhibit A in the name of and executed by Customer and accepted by InfoVision which specifies the Services, and any Support Services and/or Professional Services to be provided by InfoVision subject to the terms of this Agreement.

"**InfoVision Written Materials**" means, collectively, the Data Processing Agreement, the applicable versions of all Policies, Terms, and any other InfoVision documents that are referenced in, or on the Platform, or incorporated into, Customer's Order Form for Services.

"**Personal Information**" means information defined as personally identifiable, personal information or personal data by the Rules.

"**Professional Services**" means Training Services (as defined below) and the general consulting, implementation and/or training services to be provided to Customer pursuant to the term hereof, and an Order Form, as applicable.

"**Advanced Customer Support**" is a managed service available for purchase on a subscription basis. Advanced Customer Support is provided by InfoVision for a fee to assist customers in their use of the Services or specific components of the Services.

"**Platform Improvement & Security Purpose**" means InfoVision's access, storage, and responsible use of Customer Data and Author Data for the following Business Purposes (as defined by the Rules): to analyze, develop, improve, and optimize the use, function and performance of the Platform and the Services for enhanced customer experience; to ensure the security and integrity of the Platform, networks, and, systems as well as the products and Services InfoVision provides to its Customers; and to comply with applicable laws and regulations while operating its business in a transparent and compliant manner.

"**Rules**" means all applicable privacy, electronic communications, and data protection laws, rules, regulations, including Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 20216 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Services**" means, collectively, the AlphaMetricx, the online platform services from InfoVision ("Platform"), Platform is powered by Artificial Intelligence ("AI") that is procured by Customer from InfoVision in the Order Form and any subsequent Order Form from time to time, including associated offline components, third party tools/applications, Support Services and Professional Services. More information on responsible AI usage is provided in the InfoVision AI Usage Policy ("AI Usage Policy") available at Website at https://www.alphametricx.com/legal.

"**Support Services**" means the (i) supplemental, technical support services provided as specified by InfoVision in the applicable Order Form and/ or (ii) Advanced Customer Support. Support Services are provided pursuant to the terms of this Agreement and may be subject to additional fees as specified in the applicable Order Form.

"**Third Party Applications/Tools**" means all applications, tools, integrations, connectors, services (including implementation and/or customization), software, data, text, images, audio, video, photographs and other content and material, in any format, that are obtained or derived from third party sources outside of InfoVision that Customer may access through, within, or in conjunction with Customer's use of the Platform and Services.

"**Training Services**" means the training services provided as mentioned in the Order Form.

"**Users**" means individuals who are authorized by Customer to use the Platform and Services pursuant to this Agreement or as otherwise defined, restricted or limited in an Order Form or amendment to this Agreement, users may include but are not limited to Customer's employees, consultants, contractors and agents.

"**User Guide**" mean the online English Language user guides for the Platform and Services, accessible via Website at https://www.alphametricx.com/faq

"**URL Terms**" means the term with which Customer must comply, which are located at a URL, referenced in this Agreement and are hereby incorporated by reference.

"**Website**" means https://alphametricx.com & https://www.InfoVision.com/.

Exhibits.

The following exhibits are attached to and incorporated into this Agreement

- **Exhibit A**: Data Processing Agreement ("DPA") – Detailing the terms related to data processing, data protection, and cross-border data transfers.
- **Exhibit B**: Privacy Policy – Specifying the Customer's rights regarding the collection, use, and protection of personal data.
- **Exhibit C**: Cookie Policy – Detailing the use of cookies and tracking technologies, including consent management and user rights.
- **Exhibit D**: Terms and Conditions – Outlining the standard terms and conditions governing the use of the Service Provider's products and services.
- **Exhibit E**: AI Usage Policy - Outlining the guidelines and limitations for AI usage, including data handling, transparency, and compliance.

1. **Services.** Subject to the terms and condition of this Agreement, Customer shall have the non-exclusive, worldwide, limited right to use the InfoVision's Platform and its Services, ordered by Customer during the applicable period set forth in Customer's applicable Order Form for each of the Services ("Term") solely for the internal business operations of Customer. Customer may allow its Users to use the Services for this purpose, and Customer is responsible for its Users' compliance with this Agreement and Customer's applicable Order Form. The term of this Agreement shall also apply to updated and upgrades subsequently provided by InfoVision to Customer for the Services.

2. **Order Forms.** The Services shall be ordered by the Customer pursuant to Order Forms. Each Order Form shall include a list of Services being ordered and the associated fees.

3. **Restrictions.**

3.1 General Restrictions.

3.1.1. Customer may not, and may not cause, aid, abet or permit others to: (a) use the Services to harass any person; cause damage or injury to any person or property; publish any material that is false, defamatory, harassing or obscene; violate privacy rights; promote bigotry, racism, hatred or harm; send unsolicited bulk e-mail, junk mail, spam or chain letters; infringe property rights; sell, manufacture, market and/or distribute any product or service in violation of applicable laws; or otherwise violate applicable laws, ordinances or regulations; (b) perform or disclose any benchmarking, availability or performance testing of the Services on the Platform; or (c)perform or disclose any performance or vulnerability testing of the Services on the Platform without InfoVision's prior written approval. The Customer is permitted to access and utilize the Platform solely through an InfoVision Account. The Customer agrees to provide and maintain accurate and up-to-date information for their InfoVision Account. The Customer is responsible for adding and managing authorized users within their InfoVision Account, safeguarding the confidentiality of all InfoVision Account passwords, ensuring that each password is utilized exclusively by the authorized user, and preventing the sharing of InfoVision Accounts and passwords. Customer must also maintain the security of their InfoVision Account and any equipment used to connect to, access, or utilize the Platform and the Connected Services. Access to the Platform shall be strictly limited to authorized individuals, and Customer agrees to promptly disable access to the InfoVision Account for any employee, contractor, or representative who is no longer authorized to use the Platform (the "Acceptable Use Policy"). In addition to other Rights that InfoVision has in this Agreement and Customer Order Form, InfoVision has the right to take remedial action if the Acceptable Use Policy is violated, and such remedial action may include, without limitation, removing or disabling access to the Platform that violates the Acceptable Use Policy and/or terminating the Customer's Service.

3.1.2. Customer may not, and may not cause or permit others to: (a) modify, make derivative works of, disassemble, decompile, reverse engineer, reproduce, republish, download, or copy any part of the Services (including data structures or similar materials produced by programs); (b) access or use the Services to build or support, directly or indirectly, products or services competitive to InfoVision; or (c) license, sell, transfer, assign, distribute, outsource, permit timesharing or service bureau use of, commercially exploit, or make available the Services to any third party except as permitted by this Agreement or Order Form.

3.2 HIPAA. Unless otherwise specified in Customer Order Form, Customer agrees that: (i) InfoVision is not acting on Customer's behalf as a Business Associate or Subcontractor; (ii) the Services may not be used to store, maintain, process or transmit protected health information ("PHI") and (iii) the Services will not be used in any manner that would require InfoVision or the Services to be compliant with the Health Insurance Portability and Accountability Act of 1996, as amended and supplemented ("HIPAA"). As mentioned in the preceding sentence, the terms "Business Associate", "Subcontractor", "protected health information" or "PHI" shall have the meanings described in HIPAA.

4. Term, Fee, Payment & Taxes.

4.1 Term. This Agreement is valid for the Order Forms which this Agreement accompanies. The initial subscription period of the Services procured by the Customer shall continue for the Term applicable to such Services specified in the applicable Order Form. In the event that all of Customer's orders for Services placed under this Agreement expire or terminate, this Agreement shall similarly expire or terminate. If Customer has not entered into an Order Form with InfoVision regarding renewal of Customer's Services prior to the expiration of the initial Term or then-current renewal Term of such Services, then the subscription term of such Services shall be automatically renewed for one (1) year unless and until either party provides written notice of non-renewal to the other at least thirty (30) days before expiration of the applicable initial Term or then-current renewal Term. For the avoidance of doubt, such auto-renewals shall not apply to Professional Services unless (a) Professional Services are for training subscription(s) or (b) expressly specified in the Order Form for such Professional Services.

4.2 Fees and Payments. All fees payable is due within thirty (30) days from the invoice date unless otherwise specified in the applicable Order Form. Except as otherwise provided on the Order Form or this Agreement, once placed, each Order Form is non-cancellable, and all sums paid are non-refundable.

4.3 Taxes. InfoVision fees do not include any local, state, federal or foreign taxes, levies or duties of any nature, including value-added, sales use or withholding taxes ("Taxes"). The customer is responsible for paying all Taxes, excluding only taxes based on InfoVision's net income. If InfoVision has the legal obligation to pay or collect Taxes for which Customer is responsible under this Section, the appropriate amount shall be invoiced to and paid by Customer unless Customer provides InfoVision with a valid tax exemption certificate authorized by the appropriate taxing authority.

5. Proprietary Rights.

5.1 Ownership of Author Data. All rights, title, and interest in and to the Author Data remain with the respective Content Authors who publish such data on publicly available platforms. InfoVision does not claim ownership over Author Data but processes it in accordance with the Platform Author Privacy Policy available at _____. The collection, indexing, and use of Author Data are subject to the terms outlined in the Author Privacy Policy, ensuring compliance with applicable data protection laws and ethical data usage standards.

5.2 Ownership of Customer Data. As between InfoVision and Customer, all title and intellectual property rights in and to the Customer Data is owned exclusively by the Customer. Customer acknowledges and agrees that in connection with the provision of the Services, InfoVision may store and maintain Customer Data for a period of time consistent with InfoVision's standard business processes for the Services. Following expiration or termination of the Agreement or a Customer account, InfoVision will deactivate the applicable Customer account(s) and delete any data therein. Customer grants InfoVision the right to host, use, process, display and transmit Customer Data to provide the Services pursuant to and in accordance with this Agreement and the applicable Order Form. Customer has sole responsibility for the accuracy, quality, integrity, legality, reliability, and appropriateness of Customer Data, and for obtaining all rights related to customer Data required by InfoVision to perform the Services.

5.3 InfoVision Intellectual Property Rights. All rights, title and interest in and to the Services (including without limitation all intellectual property rights therein and all modifications, extensions, customizations, scripts or other derivates works of the Services provided or developed by InfoVision) and anything developed or delivered by or on behalf of InfoVision under this Agreement (including without limitation, Deliverables and Platform) are owned exclusively by InfoVision or its licensors. Except as provided in this Agreement, the rights granted to Customer do not convey any rights in the Services, express or implied, or ownership in the Services or any intellectual property rights thereto. Customer grants InfoVision a royalty free, worldwide, perpetual, irrevocable, transferable right to use, modify, distribute and incorporate into the Services (without attribution of any kind) any suggestions, enhancement request, recommendations, proposals, correction or other feedback or information provided by Customer or any Users related to the operation or functionality of the Services. Any rights in the Services or InfoVision's intellectual property not expressly granted herein by InfoVision are reserved by InfoVision. InfoVision, its Platform's service marks, logos and product and service names are marks of InfoVision ("InfoVision Marks"). Customer agrees not to display or use the InfoVision Marks in any manner without InfoVision's express prior written permission. The trademarks, logos and service marks of Third-Party Application/Tool providers ("Marks") are the property of such third parties. Customer is not permitted to use these Marks without the prior written consent of such third party which may own the Mark.

6. Terms of Service.

6.1 Accuracy of Customer's Contact Information. Customer shall provide accurate, current and complete information on Customer's legal business name, address, email address and phone number, and maintain and promptly update this information if it should change.

6.2 Notice. Any notice required under this Agreement shall be provided to the other party in writing. If customer has a legal dispute with InfoVision or if Customer wishes to provide a notice under the Indemnification Section of this Agreement, or if Customer becomes subject to insolvency or other similar legal proceedings, Customer will promptly send written notice to:

InfoVision, Inc.
Attention: Rajesh Kari
800 E Campbell Rd, Suite 388
Richardson, Texas -75081

6.3 Third-Party Applications/Tools.

6.3.1 The Services may enable Customer to link to, transfer Author Data to, or otherwise access, Third-Party Applications/Tools. InfoVision does not control and is not responsible for Third Party Applications/tools, regardless of whether or not such Third-Party Applications/tools are provided by a third party to which InfoVision is member of their partner program or they are member of InfoVision's partner program or otherwise designated by InfoVision "certified", "approved" or recommended. If Customer is using Third Party Applications/tools with the Services, Customer agrees that InfoVision may enable such third party providers to access Customer Data and Author Data for the interoperation of such Third Party Applications/Tools with the Services, and any exchange of data or other interaction between Customer and a third party provider is solely between Customer and such third party provider pursuant to a separate privacy policy or other terms governing Customer's access to or use of the Third Party Applications/Tools. Customer is solely responsible for complying with the terms of access and use of Third-Party Applications/Tools, and if InfoVision accesses or uses any Third Party Applications/Tools on Customer's behalf to facilitate performance of the Services, Customer is solely responsible for ensuring that such access and use, including through passwords, credentials or tokens issued or otherwise made available of Customer, is authorized by the terms of access and use for such services. If Customer transfers or causes the transfer of Customer Data and Author Data from the Platform to a Third-Party Application/Tool or other location, that transfer constitutes a distribution by Customer and not by InfoVision.

6.3.2 Any Third-Party Applications/Tools InfoVision makes accessible are provided on an "as-is" and "as available" basis without any warranty of any kind. InfoVision disclaims all liabilities arising from or related to Third Party Applications/Tools. InfoVision shall not be responsible for any

disclosure, modification or deletion of Customer Data or Author Data resulting from any such access by Third Party Applications/Tools or third-party providers. No procurement of such Third-Party Applications/Tools is required to use the Platform.

6.3.3 Customer acknowledges that: (a) the nature, type, quality and availability of Third-Party Applications/Tools may change at any time during the term, and (b) features of the Platform that interoperate with Third Party Applications/Tools may depend on the continuing availability of such Third-Party Applications/Tools. Any change to Third Party Applications/Tools, including their unavailability, during the Term does not affect Customer's obligation under this Agreement, including but not limited to User names and email addresses, support cases and billing/payment information.

6.4 Support Services, Professional Services and Training Services.

6.4.1 Support Services. As part of the Services, InfoVision will provide Customer with Help Documentation and other resources to assist Customer in its use of the Platform.

6.4.2 Professional Services. InfoVision offers Professional Services. InfoVision will provide the Customer with Professional Services as set forth in an Order Form executed by the Customer and accepted by InfoVision. All Order Forms are subject to the terms of this Agreement.

6.4.3 Training Services. All training services, including any Deliverables, are provided for Customer's internal training purposes only. Customer may not replicate Deliverables or use Deliverables to develop any of the products described in such training Deliverables. Training Deliverables are not subject to any maintenance, support, or updates.

6.5 Updates. During the Term, InfoVision may update the Services to reflect changes in, among other things, laws, regulations, rules, technology, industry practices, patterns of system use, and availability of Third-Party Applications. InfoVision updates to the Services will not materially reduce the level of performance, functionality, security or availability of Services during the Term.

6.6 Service Monitoring, Analysis, Platform Improvement & Security Purpose

6.6.1 InfoVision continuously monitors the Services to facilitate InfoVision's operation of the Services; to help resolve Customer service requests; to detect and address threats to the functionality, security, integrity, and availability of the Services as well as any content, data, or applications in the Services; and to detect and address illegal acts or violations of the Acceptable Use Policy. InfoVision monitoring tools do not collect or store any Author Data or Customer Data residing in the Services, except as needed for such purposes. Information collected by InfoVision

monitoring tools, if applicable (excluding Customer Data) may also be used to assist in managing InfoVision's product and service portfolio, to help InfoVision address deficiencies in its product and service offerings, and for license management purposes.

6.6.2 InfoVision may (i) compile statistical and other information related to the performance, operation and use of the Platform, and (ii) use data from the Services in aggregated form for security and operations management, to create statistical analysis, and for research and development purposes (clause (i) and (ii) are collectively referred to as "Service Analysis").

6.6.3 InfoVision may access, use, store, process, and analyze Customer Data, which may include Personal Data, for the Platform Improvement & Security Purpose when the Platform Improvement & Security Purpose is compatible with the original purpose of processing as determined by InfoVision. InfoVision's controlling and processing of Customer Data for the Platform Improvement & Security Purpose shall be conducted in accordance with applicable laws and contractual obligations.

6.6.4 Customer may submit a written notice to InfoVision to cease using Customer Data for the Platform Improvement & Security Purpose, InfoVision may for a reasonable period of time after the notice, continue to access, store, and use Customer Data for the Platform Improvement & Security Purpose (the "Continued Rights Period"). Customer and InfoVision agree to continue to comply with the Rules during the Continued Rights Period. At the end of the Continued Rights Period, InfoVision will delete or render Customer Data unrecoverable in accordance with the Rules.

6.7 Security. InfoVision shall maintain commercially reasonable administrative, physical, and technical safeguards designed to protect the confidentiality, integrity, and availability of Customer Data. These safeguards include, but are not limited to, encryption, access controls, intrusion detection systems, regular vulnerability assessments, and secure data storage and transmission protocols. Additional details regarding these measures are provided in the Data Processing Agreement (Exhibit A), which is incorporated by reference into this Agreement.

6.8 Data Protection for Services

6.8.1 The Data Processing Agreement (Exhibit A), governs the processing of Personal Data in connection with the Services and is hereby incorporated by reference. The terms of the Data Processing Agreement shall prevail over any conflicting provisions in this Agreement regarding data protection and privacy obligations.

6.8.2 In performing the Services, InfoVision will comply with its Platform's Privacy Policy, which is available at Website at https://alphametricx.com/privacy-policy and incorporated herein by reference. The Privacy Policy is subject to change at InfoVision's discretion; however, InfoVision policy changes will not result in a material reduction in the level of protection provided for

Customer's Personal Data (as defined in InfoVision's Data Processing Agreement) provided as part of Customer Data during the Term.

6.8.3 Unless otherwise provided in the applicable Order Form, the version of InfoVision's Data Processing Agreement for the Services (the "**Data Processing Agreement**") applicable to Customer's Order Form, as of the Order Form Effective Date, and is incorporated herein by reference, will remain in force during the Term specified in Customer's Order Form. The Data Processing Agreement describes the parties' respective roles for the processing and control of Personal Data that Customer provides to InfoVision as part of the Services. Unless otherwise provided in the applicable Order Form, InfoVision will act as a data processor, controller, sub-processor and will act on Customer Instructions concerning the treatment of Customer's Personal Data residing in the services environment, as specified in this Agreement, the Data Processing Agreement and the applicable Order Form respectively. Customer agrees to provide any notices and obtain any consents related to Customer's use of Services and InfoVision's provision of the Services, including those related to the collection, use, processing, transfer and disclosure of Personal Data.

6.8.4 The Data Processing Agreement does not apply to any (1) demonstration accounts, trials, beta releases, or other similar versions of the Services; or (2) the processing of Personal Data for the Platform Improvement & Security Purpose.

6.9 Data Protection for Platform Improvement & Security Purpose

6.9.1 Personal Data. The parties agree that Customer Data may include Personal Data. Each party is a Data controller (as defined in the Rules) with regard to the use and processing of Customer Data for the Platform Improvement & Security Purpose permitted in this Agreement. Each party is responsible for its controller obligations, including notice requirements, under the Rules.

6.9.2 Lawful Basis for Processing. InfoVision will process Personal Data for the Platform Improvement & Security Purpose based on InfoVision's legitimate interests when such processing has been determined solely by InfoVision to have a limited privacy impact on the individual or as necessary for compliance with InfoVision legal obligations.

6.9.3 Compliance with Rules. InfoVision will comply with the Rules applicable to InfoVision in its role of providing Customer the Services. Customer will comply with the Rules that apply to Customer's use of the Services, including the collection, use, and sharing of Customer Data with InfoVision. Customer and InfoVision agree to negotiate in good faith to amend this Agreement as may be necessary to comply with changes to the Rules.

6.9.4 Sensitive Data Prohibition. InfoVision will not knowingly process Customer Data that contains Personal Data of children under 16 years of age or Personal Data that is "sensitive" or "special" under applicable data protection laws for the Platform Improvement & Security Purpose. InfoVision will not use the Personal Data processed for the Platform Improvement & Security Purpose to make decisions solely by automatic means where the decision has a legal or significant effect on the individual, or in any way or does discriminate against any person or promote bigotry, racism or harm.

6.9.5 Transfer of Personal Data. InfoVision may store or transfer Customer Data on a global basis as necessary for the Platform Improvement & Security Purpose. InfoVision and its affiliates may perform certain aspects of the Services (e.g. administration, maintenance, support, disaster recovery, data processing, etc.) from locations and through subcontractors, worldwide. Data transfers are made subject to the terms of the EU Standard Contractual Clauses for Controllers ("**Clauses**") if: (a) Customer share, use, or process Personal Data under this Agreement; and (b) such data transfer is: (i) subject to any restrictions or requirements under Directive 95/46/EC or Regulation (EU) 2016/676 repealing Directive 95/46/EC (General Data Protection Regulation); and (ii) made to countries, jurisdictions or recipients outside the EEA or Switzerland not recognized by the European Commission as ensuring an adequate level of protection pursuant to Directive 95/46/EC or General Data Protection Regulation. Customer and InfoVision agree that incorporation of the Clauses into this Agreement acts as a legally binding execution of the Clauses as entered into between InfoVision (acting in its own name and in the name and on behalf of the InfoVision Affiliates) and Customer (acting in Customer's own name and in the name and on behalf of Customer's affiliates).

7. Suspension/Termination.

7.1 Suspension for Delinquent Account. InfoVision reserves the right to suspend the Customer's access to and/or use of the Services for any reason including but not limited to if any payment is due but unpaid.

7.2 Suspension for Ongoing Harm. InfoVision may suspend Customer's or User's access to, or use of, the Services, including without limitation, Platform Services, if InfoVision believes that (a) there is a significant threat to the functionality, security, integrity, or availability of the Services or any content, data, or applications in the Services; (b) Customer or Users are accessing or using the Services to commit an illegal act; or (c)there is a violation of the Acceptable Use Policy. When reasonably practicable and lawfully permitted, InfoVision will provide the Customer with advance notice of any such suspension. InfoVision will use reasonable efforts to re-establish the Services promptly after InfoVision determines that the issue causing the suspension has been resolved. During any suspension period, InfoVision will make Customer Data or Author Data (as it existed on the suspension date) available to the

Customer. Any suspension under this Section shall not excuse Customer from Customer's obligation to make payments under this Agreement.

7.3 Termination for Cause. If either Customer or InfoVision breached a material term of this Agreement or any Order Form and fails to correct the breach within thirty (30) days of written specification of the breach, then the breaching party is in default and the non-breaching party may terminate (a) in the case of breach of any Order Form, the Order Form under which the breach occurred; or (b) in the case of breach of the Agreement, the Agreement and all Order Forms that have been placed under the Agreement. If InfoVision terminates any orders as specified in the preceding sentence, Customer must pay within 30 days all amount that have accrued prior to such termination, as well as all sums remaining unpaid for the Services under such Order Forms plus related taxes and expenses. Further, in case of advance payments, no amount shall be refunded. Except for nonpayment of fees, the non-breaching party may agree in its sole discretion to extend the thirty (30) day period for so long as the breaching party continues reasonable efforts to cure the breach. Customer agrees that if it is in default under this Agreement, Customer may not use those Services ordered.

7.4 Customer agrees that InfoVision shall not be liable to Customer or other third party for any suspension pursuant to this Section 7.

8. Confidentiality.

8.1 By virtue of this Agreement, the parties may disclose to each other information that is confidential ("Confidential Information"). Confidential Information shall be limited to the terms and pricing under this Agreement and Customer's Order Forms, Customer Data residing in the Services, and all information clearly identified as confidential at the time of disclosure.

8.2 A party's Confidential Information shall not include information that: (a) is or becomes a part of the public domain through no act or omission of the other party; (b) was in the other party's lawful possession prior to the disclosure and had not been obtained by the other party either directly or indirectly from the disclosing party; (c) is lawfully disclosed to the other party by a third party without restriction on the disclosure; or (d) is independently developed by the other party.

8.3 Each party agrees not to disclose the other party's Confidential Information to any third party other than as set forth in the following sentence for a period of five years from the date of the disclosing party's disclosure of the Confidential Information to the receiving party; however, InfoVision will protect the confidentiality of Customer data residing on the Platform for as long as such information resides on the Platform. Each party may disclose Confidential Information only to those employees, agents or subcontractors who are required to protect it against

unauthorized disclosure in a manner no less protective than required under this Agreement, and each party may disclose the other party's Confidentiality of Customer Data residing on the Platform in accordance with the InfoVision security practices applicable to Customer's Order Form as described in this Agreement or such Order Form.

9. Warranties, disclaimers and Exclusive Remedies

9.1 Each party represents that it has validly entered into this Agreement and that it has the power and authority to do so. InfoVision warrants that during the Term, InfoVision will perform (i) the services of the Platform using commercially reasonable care and skill in all material respects as described in the Written Materials, and (ii) any Professional Services and Support Services in a professional manner consistent with industry standards (the warranties described by the forgoing clauses (i) and (ii), collectively, the "Service Warranty"). If the Services provided to the Customer were not performed as warranted, Customer must promptly provide InfoVision with a written notice that describes the deficiencies in the Services. For Professional Services, Customer must notify InfoVision of any warranty deficiencies within 60 days from performance of the deficient Professional Services.

9.2 INFOVISION DOES NOT WARRANT THAT THE SERVICES WILL BE PERFORMED ERROR-FREE OR UNINTERRUPTED, THAT INFOVISION WILL CORRECT ALL SERVICES ERRORS, OR THAT THE SERVICES WILL MEET CUSTOMER'S REQUIREMENTS OR EXPECTATIONS. INFOVISION IS NOT RESPONSIBLE FOR ANY ISSUES RELATED TO THE PERFORMANCE, OPERATION OR SECURITY OF THE SERVICES THAT ARISE FROM CUSTOMER DATA, AUTHOR DATA OR THIRD-PARTY APPLICATIONS OR SERVICES PROVIDED BY THE THIRD PARTIES.

9.3 FOR ANY BREACH OF THE SERVICES WARRANTY, CUSTOMER'S EXCLUSIVE REMEDY AND INFOVISION'S ENTIRE LIABILITY SHALL BE THE CORRECTION OF THE DEFICIENT SERVICES THAT CAUSED THE BREACH OF WARRANTY, OR IF INFOVISION CANNOT SUBSTANTIALLY CORRECT THE DEFICIENCY IN A COMMERCIALLY REASONABLE MANNER, CUSTOMER MAY END THE DEFICIENT SERVICES AND INFOVISION WILL REFUND TO CUSTOMER THE FEES FOR THE TERMINATED SERVICES THAT CUSTOMER PRE-PAID TO INFOVISION FOR THE PERIOD FOLLOWING THE EFFECTIVE DATE OF TERMINATION.

9.4 TO THE EXTENT NOT PROHIBITED BY LAW, THESE WARRANTIES ARE EXCLUSIVE AND THERE ARE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS INCLUDING FOR SOFTWARE, HARDWARE, SYSTEMS, NETWORKS, ENVIRONMENTS OR FOR MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE.

10. Limitations of Liability.

10.1 IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES BE LAIBLE FOR ANY INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES, OR ANY LOSS OF REVENUE, PROFITS (EXCLUDING FEES UNDER THIS AGREEMENT), SALES, DATA, DATA USE, GOODWILL, OR REPUTATION.

10.2 IN NO EVENT SHALL THE AGGREGATE LIABILITY OF INFOVISION AND ITS AFFILIATES ARISING OUT OR RELATED TO THIS AGREEMENT OR CUSTOMER'S ORDER FORM, WHETHER IN CONTRACT, TORT, OR OTHERWISE, EXCEED THE TOTAL AMOUNTS ACTUALLY PAID UNDER CUSTOMER'S ORDER FORM FOR THE SERVICES GIVING RISE TO THE LIBAILITY DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH LIABILITY.

11. Indemnification.

11.1 If a third party makes a claim against either Customer or InfoVision ("Recipient" which may refer to Customer or InfoVision depending upon which party received the Material), that any information, design, specification, instruction, software, service, data, hardware, or material (collectively, "Material") furnished by either Customer or InfoVision ("Provider" which may refer to Customer or InfoVision depending on which party provided the Material) and used by the recipient infringes the third party's intellectual property rights or violates the third party's data privacy rights, the Provider, at the Provider's sole cost and expense, will defend the recipient against the claim and indemnify the Recipient from the damages, liabilities, costs and expenses awarded by the court to the third party claiming infringement or the settlement agreed to by the Provider, if the recipient does the following:

a. Notifies the Provider promptly in writing, not later than thirty (30) days after the Recipient received notice of the claim (or sooner if required by applicable law);

b. Gives the Provider sole control of the defense and any settlement negotiations; and

c. Gives the Provider the information, authority and assistance the Provider needs to defend against or settle the claim.

11.2 If the Provider believed or it is determined that any of the Material may have violated a third party's intellectual property rights, the Provider may choose to either modify the Material to be non-infringing (while substantially preserving its utility or functionality) or obtain a license to allow for continued use, or if these alternatives are not commercially reasonable, the Provider may end the license for, and require return of, the applicable Material and refund any unused, prepaid fees the Recipient may have paid to the other party for such Material. If such a return materially affects InfoVision's ability to meet obligations under the relevant order, then InfoVision may, upon thirty (30) days prior written notice, terminate the order. If such Material is third party technology and the terms of the third-party license do not allow us to terminate the license, then InfoVision may, upon thirty (30) days prior written notice, end the Services associated with such Material and refund any unused, prepaid fees for such Services.

11.3 The Provider will not indemnify the Recipient if the Recipient (a) alters the Material or uses it outside the scope of use identified in the Provider's user or program documentation or the User Guides, or (b) uses a version of the Material which has been superseded, if the infringement claim could have been avoided by using an unaltered current version of the Material which was made available to the Recipient. The Provider will not indemnify the Recipient to the extent that an infringement claim is based upon any Material not furnished by the Provider. InfoVision will not indemnify Customer to the extent that an infringement claim is based on the Third Party Application/Tool or any Material from a third party portal or other external source that is accessible or made available to Customer within or by the Services (e.g., a social media post from a third party blog or forum, a third party Web page accessed via a hyperlink, marketing data from third party data providers, etc.)

11.4 This Section 11 provides the parties' exclusive remedy for any infringement claims or damages.

12. Governing Law and Jurisdiction. This Agreement is governed by the substantive and procedural laws of the State of Texas and each party agrees to submit to the exclusive jurisdiction of, and venue in the courts of the State of Texas in any dispute arising out of or relating to this Agreement. The Uniform Computer Information Transactions Act does not apply to this Agreement or to orders placed under it.

13. Export.

13.1 Export laws and regulations of the United States and any other relevant local export laws and regulations apply to the Services. Such export laws govern use of the Services (including technical data) and any Services deliverables provided under this Agreement, and Customer and InfoVision each agree to comply with all such export laws and regulations (including "deemed export" and "deemed re-export" regulations). Customer agrees that no data,

information, software programs and/or materials resulting from the Services (or direct Platform thereof) will be exported, directly or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation, or development of missile technology.

13.2 Customer acknowledges that the Services are designed with capabilities for Customer and Customer Users to access the Services without regard to geographic location and to transfer or otherwise move Author Data and Customer Data between the Services and other locations such as User workstations. Customer is solely responsible for the authorization and management of User accounts across geographic locations, as well as export control and geographic transfer of Author Data and Customer Data.

14. General Provisions.

14.1 Entire Agreement.

14.1.1. This Agreement incorporates by reference all URL Terms (as applicable), Exhibits and Order Forms, and this Agreement, together with such referenced items, constitute the entire understanding between Customer and InfoVision and are intended to be the final and entire expression of their agreement. The parties expressly disclaim any reliance on any and all prior discussions, emails, RFP's and/or agreements between the parties. There are no other verbal agreements, representations, warranties undertakings or other agreements between the parties.

14.1.2. Under no circumstances will the terms, conditions or provisions of any purchase order, invoice or other administrative document issued by Customer in connection to this Agreement be deemed to modify, alter or expand the rights, duties or obligations of the parties under, or otherwise modify, this Agreement, regardless of any failure of InfoVision to object to such terms, provisions, or conditions. In the event of any inconsistencies between the terms of an Order Form and the Agreement, the Order Form shall take precedence; however, unless expressly stated otherwise in an Order Form, the terms of the Data Processing Agreement shall take precedence over any inconsistent terms in an Order Form.

14.1.3. The Agreement shall not be modified, or amended, except as expressly set forth herein, or in writing and signed or accepted electronically by the party against whom the modification, amendment or waiver is to be asserted, or by a properly executed Order Form.

14.2 Other General Provisions.

14.2.1. This Agreement shall inure to benefit and bind the parties hereto, their successors and assigns. Customer may not assign this Agreement or give or transfer the Services or any interest in the Services to another individual or entity. There are no third-party beneficiaries to this Agreement.

14.2.2. InfoVision is an independent contractor, and each party agrees that no joint venture, partnership, or agency relationship exists between the parties.

14.2.3. InfoVision's business partners and other third parties, including any third parties with which the Services have integrations or that are retained by Customer to provide consulting services, implementation services or applications/tools that interact with the Services, are independent of InfoVision and are not InfoVision's agents. InfoVision makes no representation or warranty about the suitability of any InfoVision business partner or any third party in connection with the provision of consulting services, implementation services or applications/tools.

14.2.4. If any provision is held by a court of competent jurisdiction to be contrary to law, such provision shall be eliminated or limited to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect. A waiver of any breach under this Agreement should not constitute a waiver of any other breach or future breach.

14.2.5. Force Majeure. Neither party shall be liable for loss, delay, nonperformance (including failure to meet the service level commitment but excluding payment obligations) to the extent resulting from any force majeure event, including, but not limited to, acts of God, strike, riot, fire, explosion, flood, earthquake, natural disaster, terrorism, act of war, civil unrest, criminal acts of third parties, failure of the internet, governmental acts or orders or restrictions, failure of suppliers, labor stoppage or dispute (other than the involving InfoVision employees), or shortage of materials, provided that such party uses reasonable efforts, under the circumstances, to notify the other party of the circumstances causing the delay and to resume performance as soon as possible and any delivery date shall be extended accordingly.

14.2.6. Non-Impediment. Nothing in this Agreement shall be construed as precluding or limiting in any way the right of InfoVision to provide consulting, development, or other services of any kind to any individual or entity (including without limitation performing services or developing materials which are similar to and/or competitive with the Professional Services and/or Deliverables hereunder).

14.2.7. Audit. Upon forty-five (45) days written notice and no more than once every twelve (12) months, InfoVision may audit Customer's use of the Services to ensure Customer's use of the Platform is in compliance with the terms of the applicable Order Form and this Agreement. Any such audit shall not unreasonably interfere with Customer's normal business operations. Customer agrees to cooperate with InfoVision's audit and to provide reasonable assistance and access to

information reasonably requested by InfoVision. The performance of the audit and non-public data obtained during audit (including findings or reports that result from the audit) shall be subject to the provisions of Section 8 (Confidentiality) of this Agreement. If the audit identifies non-compliance, the Customer agrees to remedy (which may include, without limitation, the payment of any fees for additional Services) such non-compliance within thirty (30) days of written notification of that non-compliance. The customer agrees that InfoVision shall not be responsible for any of the Customer's costs incurred in cooperating with the audit.

14.2.8. The Section headings used in this Agreement are included for reference purposes only and shall not affect the meaning or interpretation of this Agreement in any way. Provisions that survive termination or expiration of this Agreement are those relating to limitation of liability, indemnification, payment and others which by their nature are intended to survive. This Agreement may be executed in counterparts and/or by facsimile or electronic signature and if so, executed shall be equally binding as an original copy of this Agreement executed in ink by both parties.

Exhibit A

Data Processing Agreement ("DPA")

This DPA is incorporated into and forms an integral part of the Agreement entered into between InfoVision (the "Service Provider") and the Customer, as identified in the applicable order. Terms not defined in this DPA shall have the meanings assigned to them in the Agreement.

1. Definitions

1.1 "**Applicable Data Protection Law**" means all data privacy or data protection laws or regulations globally that apply to the Processing of Personal Information under this Data Processing Agreement, including Applicable European Data Protection Law, Applicable UK Data Protection Law, the California Consumer Privacy Act as amended ("CCPA") and other US State laws.

1.2 "**Applicable European Data Protection Law**" means (i) the EU General Data Protection Regulation EU/2016/679, as supplemented by applicable EU Member State law and as incorporated into the EEA Agreement; and (ii) the Swiss Federal Act of 19 June 1992 on Data Protection, as amended.

1.3 **"Applicable UK Data Protection Law"** means (i) the UK GDPR, meaning the EU General Data Protection Regulation EU/2016/679, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 pursuant to amendments to the EU General Data Protection Regulation EU/2016/679 made by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020; and (ii) the UK Data Protection Act 2018, as amended.

1.4 "**Europe"** means for the purposes of this Data Processing Agreement (i) the European Economic Area, consisting of the EU Member States, Iceland, Liechtenstein and Norway; and (ii) Switzerland.

1.5 "**Individual"** shall have the same meaning as the term "data subject" or the equivalent term under Applicable Data Protection Law.

1.6 "**Information Breach"** means a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Your Content transmitted, stored or otherwise Processed on Service Provider systems or the Services environment that compromises the security, confidentiality or integrity of Your Content.

1.7 "**Process/Processing**", "**Controller**", "**Processor**" and "**Binding Corporate Rules**" (or the equivalent terms) have the meaning set forth under Applicable Data Protection Law.

1.8 **"Service Provider", "Sell", "Share", "Business Purpose",** and **"Commercial Purpose"** have the meaning set forth under the CCPA.

1.9 "**Service Provider Affiliate(s)**" means the subsidiar(y)(ies) of InfoVision, Inc. that may Process Personal Information as set forth in this Data Processing Agreement.

1.10 "**Service Provider Intra-Company Data Transfer and Mandate Agreement"** means the Service Provider Intra-Company Data Transfer and Mandate Agreement for Customer Services Personal Information entered into between Service Provider Corporation and the Service Provider Affiliates.

1.11 "**Service Provider Binding Corporate Rules for Processors**" or "**Service Provider Processor Code**" means the EU or UK Service Provider's Privacy Code for Processing Personal Information of Customer Individuals, as the case may be.

1.12 "**Service Provider**" means the Service Provider Entity/Affiliate that has executed the Services Agreement.

1.13 "**Personal Information**" shall have the same meaning as the term "personal data", "personally identifiable information (PII)" or the equivalent term under Applicable Data Protection Law.

1.14 "**Regulator**" shall have the same meaning as the term "supervisory authority", "data protection authority" or the equivalent term under Applicable Data Protection Law.

1.15 "**Services**" or the equivalent terms "Service Offerings" or "services" means, collectively, the AlphaMetricx, the online platform services from Service Provider ("Platform"), Support Services and Professional Services specified in the Services Agreement.

1.16 "**Services Agreement**" means (i) the applicable order for the Services you have purchased from Service Provider; (ii) the applicable agreement referenced in the applicable order, and (iii) the Service Specifications.

1.17 "**Third Party Subprocessor**" means a third party, other than the Service Provider or its Affiliate, which Service Provider subcontracts with and which may Process Personal Information as set forth in this Data Processing Agreement.

1.18 **"Customer",** "**You**" means the customer entity that has executed the Services Agreement.

Other capitalized terms have the definitions provided for them in the Services Agreement.

2. Scope and Applicability

This Data Processing Agreement applies to Service Provider's Processing of Personal Information on Your behalf as a Processor and Controller in cases of platform security, marketing, account management, etc. for the provision of the Services specified in Your Services Agreement. Unless otherwise expressly stated in Your Services Agreement, this version of the Data Processing Agreement shall be effective and remain in force for the term of Your Services Agreement. For clarity, Service Provider may act as a Controller, Processor, or Subprocessor depending on the specific circumstances and nature of the Services provided. The role of the Service Provider in relation to any particular data processing activity will be determined under Applicable Data Protection Law.

3. Responsibility for Processing and Controlling of Personal Information and Description of Processing and Controlling Activities

3.1 You are a Controller and Service Provider is a Processor for the Processing of Personal Information as part of the provision of the Services. In some instances like strengthening platform security, marketing, and account management, Service Provider can also act as a Controller. Each party is responsible for compliance with its respective obligations under Applicable Data Protection Law. Depending on the Services, Service Provider may also act as a Subprocessor where it Processes Personal Information on behalf of another Processor (e.g., a Customer's third-party vendor). In each such case, Service Provider will comply with the obligations corresponding to its role under Applicable Data Protection Law.

3.2 Service Provider will Control or Process Personal Information during the term of the Services Agreement solely for the purpose of providing the Services in accordance with the Services Agreement and this Data Processing Agreement.

3.3 In particular and depending on the Services, Service Provider may Process Personal Information for hosting and storage; backup and disaster recovery; service change management; issue resolution; applying new product or system versions, patches, updates and upgrades; monitoring and testing system use and performance; IT security purposes including incident management; maintenance and performance of technical support systems and IT infrastructure; and migration, implementation, configuration and performance testing.

3.4 As part of the provision of the Services and depending on the Services, Service Provider may Process Personal Information about Your Individuals, including Your users, employees, contractors, collaborators, partners.

3.5 Personal Information about Your Individuals may include, but is not limited to, personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords; information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, and business contact details; financial details; goods and services provided; unique IDs collected from mobile devices, network carriers or data providers; geolocation data; IP addresses and online behavior and interest data.

3.6 Unless otherwise specified in the Services Agreement, You may not provide Service Provider with any data that imposes specific data security or data protection obligations on Service Provider in addition to or different from those specified in the Data Processing Agreement or Services Agreement (e.g. certain regulated health or payment card information). If available for the Services, You may purchase additional services from Service Provider designed to address specific data security or data protection requirements applicable to sensitive or special data You seek to include in Your Content. You remain responsible for compliance with Your specific regulatory, legal or industry data security obligations which may apply to such data.

3.7 Additional or more specific descriptions of Processing activities may be included in the Services Agreement.

3.8 InfoVision is a Service Provider in respect to Personal Information processed in performance of the Services. Service Provider will not: (a) Sell or Share any Personal Information; (b) retain, use, or disclose any Personal Information (i) for any purpose other than for the Business Purposes specified in the Services Agreement, including for any Commercial Purpose, or (ii) outside of the direct business relationship between Service Provider and You; or (c) combine Personal Information received from or on behalf of You with Personal Information received from or on behalf of any third party, or collected from Service Provider's own interaction with Individuals, except to perform a Business Purpose that is permitted by the CCPA and the Services Agreement. Service Provider will notify You of its use of Service Provider Affiliates and Third Party Subprocessors in accordance with Section 5 of this Data Processing Agreement; and ensure Service Provider Affiliates and Third Party Subprocessors are subject to applicable written agreements per Section 5 of this Data Processing Agreement. The parties acknowledge that the Personal Information You disclose to

Service Provider is provided only for the limited and specified Business Purposes set forth in the Services Agreement. Service Provider shall provide the same level of protection to Personal Information as required by the CCPA and as more fully set out in the Services Agreement. You may take such reasonable steps as may be necessary (a) to remediate Service Provider's unauthorized use of Personal Information, and (b) to ensure that Personal Information is used in accordance with the terms of this Data Processing Agreement by exercising Your rights under Section 8 of this Data Processing Agreement. Service Provider shall notify You if it makes a determination that it is not able to meet its obligations under the CCPA in connection with its provision of the Services.

4. Your Instructions

4.1 In addition to Your instructions incorporated into the Services Agreement, You may provide additional instructions in writing to Service Provider with regard to Processing of Personal Information in accordance with Applicable Data Protection Law. Service Provider will promptly comply with all such instructions to the extent necessary for Service Provider to (i) comply with its Processor obligations under Applicable Data Protection Law; or (ii) assist You to comply with Your Controller obligations under Applicable Data Protection Law relevant to Your use of the Services.

4.2 Service Provider will follow Your instructions at no additional cost to You and within the timeframes reasonably necessary for You to comply with your obligations under Applicable Data Protection Law. Service Provider will immediately inform You if, in its opinion, Your instruction infringes Applicable Data Protection Law. Service Provider is not responsible for providing legal advice to You.

4.3 To the extent Service Provider expects to incur additional charges or fees not covered by the fees for Services payable under the Services Agreement, such as additional license or third-party contractor fees, it will promptly inform You thereof upon receiving Your instructions. Without prejudice to Service Provider's obligation to comply with Your instructions, the parties will then negotiate in good faith with respect to any such charges or fees.

5. Privacy Inquiries and Requests from Individuals

5.1 If You receive a request or inquiry from an Individual related to Personal Information Processed by Service Provider under the Services Agreement, including Individual requests to access, delete or erase, restrict, rectify, receive and transmit (data portability), block access to or object to Processing of specific Personal Information, You can securely access Your Services environment that holds Personal Information to address the request. Additional information on how to access the Services to address privacy requests or inquiries from

Individuals is available in the applicable Service Provider Product or Service or support contact provided for the Services.

5.2 To the extent access to the Services is not available to You or otherwise not responsive to the request or inquiry, You can submit a "service request" via applicable primary support tool or support contact provided for the Services, such as Your project manager with detailed written instructions to Service Provider on how to assist You with such request.

5.3 If Service Provider directly receives any requests or inquiries from Individuals that have identified You as the Controller, it will promptly pass on such requests to You without responding to the Individual. Otherwise, Service Provider will advise the Individual to identify and contact the relevant controller(s).

6. Service Provider Affiliates and Third Party Subprocessors

6.1 You provide Service Provider general written authorization to engage Service Provider Affiliates and Third Party Subprocessors as necessary to assist in the performance of the Services.

6.2 To the extent Service Provider engages such Third Party Subprocessors and/or Service Provider Affiliates, it requires that such entities are subject to the same level of data protection and security as Service Provider under the terms of this Data Processing Agreement and Applicable Data Protection Law. Service Provider remains responsible for the performance of the Service Provider Affiliates' and Third-Party Subprocessors' obligations in compliance with the terms of the Services Agreement.

6.3 Service Provider maintains lists of Service Provider Affiliates and Third Party Subprocessors that may Process Personal Information. These lists are available via contact provided for the Services, such as Your Service Provider project manager. To receive notice of any intended changes to these lists of Service Provider Affiliates and Third Party Subprocessors, in a subsequent "Service Provider Subprocessor Notice", the Service Provider will send to you this by e-mail upon written request.

6.4 Within thirty (30) calendar days of Service Provider providing such notice to You under Section 6.3 above, You may object to the intended involvement of a Third Party Subprocessor or Service Provider Affiliate in the performance of the Services by submitting a "service request" via contact provided for the Services, such as Your Service Provider project manager. You and Service Provider will work together in good faith to find a mutually acceptable resolution to address such objection, including but not limited to reviewing additional

documentation supporting the Third Party Subprocessor's or Service Provider Affiliate's compliance with the Data Processing Agreement or Applicable Data Protection Law, or delivering the Services without the involvement of such Third Party Subprocessor. To the extent You and Service Provider do not reach a mutually acceptable resolution within a reasonable timeframe, You shall have the right to terminate the relevant Services (i) upon serving thirty (30) days prior notice; (ii) without liability to You or Service Provider and (iii) without relieving You from Your payment obligations under the Services Agreement up to the date of termination. If the termination in accordance with this Section 6.4 only pertains to a portion of Services under an order, You will enter into an amendment or replacement order to reflect such partial termination.

7. Cross-border data transfers

7.1 For Platform Services, Personal Information will be stored in the data center region specified in Your order for such Services or, if applicable, the geographic region that You have selected when activating the production instance of such Services.

7.2 Without prejudice to Section 7.1 above, Service Provider may Process Personal Information globally as necessary to perform the Services, such as for support, incident management or data recovery purposes.

7.3 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under Applicable European Data Protection Law to countries outside Europe not covered by an adequacy decision, such transfers are subject to (i) Service Provider's Binding Corporate Rules for Processors or BCR-p (also referred to as the Service Provider Processor Code) and (ii) the terms of Module 2 (Controller to Processor) of the EU Standard Contractual Clauses 2021/914 of 4 June 2021.

7.4 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under Applicable UK Data Protection Law, to countries outside the United Kingdom not covered by an Adequacy Decision by the UK ICO, such transfers are subject to (i) the terms of Module 2 (Controller to Processor) of the EU Standard Contractual Clauses 2021/914 of 4 June 2021 as supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses version B1.0 (the "**IDTA**"), which are incorporated herein by reference; and (ii) when approved by the UK ICO, the approved UK Binding Corporate Rules for Processors, in the form that will be approved by the UK ICO for use in the UK and will be published on Service Provider's public websites. The IDTA will be read in conjunction with the Services Agreement and the Data Processing Agreement.

7.5 The parties will review any supplemental measures, which may be required based on applicable Data Protection Law for the transfer of Personal Information to countries that do not offer an adequate level of protection. The parties will work together in good faith to find a mutually acceptable resolution to address such supplementary measures, including but not limited to reviewing technical documentation for the Services, and discussing additional available technical safeguards and security services.

7.6 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under other Applicable Data Protection Laws globally, such transfers shall be subject to (i) for transfers to Service Provider Affiliates, the terms of the Service Provider Intra-Company Data Transfer and Mandate Agreement, which requires all transfers of Personal Information to be made in compliance with Applicable Data Protection Law and all applicable Service Provider security and data privacy policies and standards globally; and (ii) for transfers to Third Party Subprocessors, security and data privacy requirements consistent with the relevant requirements of this Data Processing Agreement and Applicable Data Protection Law.

8. Security and Confidentiality

8.1 Service Provider has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Information designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information. These security measures govern all areas of security applicable to the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures. Additional details regarding the specific security measures that apply to the Services You have ordered are set out in the relevant security practices for these Services available at https://trust.alphametricx.com.

8.2 All Service Provider and Service Provider Affiliates employees, and Third Party Subprocessors that Process Personal Information, are subject to appropriate written confidentiality arrangements, including confidentiality agreements, regular training on information protection, and compliance with Service Provider policies concerning protection of confidential information.

9. Audit Rights and Assistance with Data Protection Impact Assessments

9.1 You may audit Service Provider's compliance with its obligations under this Data Processing Agreement up to once per year, including inspections of the applicable Services

data center facility that hosts Personal Information. In addition, to the extent required by Applicable Data Protection Law, You or Your Regulator may perform more frequent audits.

If You engage a third-party auditor, the third party must be mutually agreed to by You and Service Provider (except if such third party is a Regulator). Service Provider will not unreasonably withhold its consent to a third-party auditor requested by You. The third party must execute a written confidentiality agreement acceptable to Service Provider or otherwise be bound by a statutory or legal confidentiality obligation.

9.2 To request an audit, You must submit a detailed proposed audit plan to Service Provider at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Service Provider will review the proposed audit plan and provide You with any concerns or questions. Service Provider will work cooperatively with You to agree on a final audit plan within a reasonable timeframe.

9.3 The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Service Provider's health and safety or other relevant policies and may not unreasonably interfere with Service Provider business activities.

9.4 Upon completion of the audit, You will provide Service Provider with a copy of the audit report, which is subject to the confidentiality terms of Your Services Agreement. You may use the audit reports only for the purposes of meeting Your regulatory audit requirements and/or confirming compliance with the requirements of this Data Processing Agreement.

9.5 Each party will bear its own costs in relation to the audit, unless Service Provider promptly informs you upon reviewing Your audit plan that it expects to incur additional charges or fees in the performance of the audit that are not covered by the fees payable under Your Services Agreement, such as additional license or third-party contractor fees. The parties will negotiate in good faith with respect to any such charges or fees.

9.6 Without prejudice to the rights granted in Section 9.1 above, if the requested audit scope is addressed in a SOC, ISO, GDPR, HIPAA or similar audit report issued by a qualified third party auditor within the prior twelve months and Service Provider provides such report to You confirming there are no known material changes in the controls audited, You agree to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.

9.7 You may also request that Service Provider audit a Third Party Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist You in obtaining a third-party audit report concerning the Third Party Subprocessor's operations) to

verify compliance with the Third Party Subprocessor's obligations.

9.8 Service Provider provides You with information and assistance reasonably necessary for You to conduct Your data protection impact assessments or consult with Your Regulator(s), by granting You electronic access to a record of Processing activities and Service Provider Product/Service privacy & security functionality guides for the Services. This information is available upon request.

10. Incident Management and Breach Notification

10.1 Service Provider has implemented controls and policies designed to detect and promptly respond to incidents that create suspicion of or indicate destruction, loss, alteration, unauthorized disclosure or access to Your Content (as such term is defined in the Services Agreement) transmitted, stored or otherwise Processed. Service Provider will promptly define escalation paths to investigate such incidents in order to confirm if an Information Breach has occurred, and to take reasonable measures designed to identify the root cause(s) of the Information Breach, mitigate any possible adverse effects and prevent a recurrence.

10.2 Service Provider will notify you of a confirmed Information Breach without undue delay but at the latest within 24 hours. As information regarding the Information Breach is collected or otherwise reasonably becomes available to Service Provider, Service Provider will also provide You with (i) a description of the nature and reasonably anticipated consequences of the Information Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; and (iii) where possible, information about the types of information that were the subject of the Information Breach. You agree to coordinate with Service Provider on the content of Your intended public statements or required notices for the affected Individuals and/or notices to the relevant Regulators regarding the Information Breach.

11. Return and Deletion of Personal Information

11.1 Upon termination or expiration of the Agreement, Service Provider shall: (a)Deactivate Customer's account(s) and delete or render unrecoverable all Personal Information stored on its systems in accordance with the timelines specified in the Services Agreement, (b)Provide Customer with a reasonable opportunity, for up to 30 days following termination or expiration, to retrieve Personal Information using available data retrieval functionality, as specified in the Services Agreement. Ensure that all Personal Information processed by any Service Provider Affiliates or Third-Party Sub-processors is similarly deleted or returned, unless otherwise required by applicable law.

11.2 Any requests for extended retention of Personal Information beyond this period must be agreed upon in writing, and additional fees may apply. Specific processes and exceptions (e.g., legal retention obligations) are detailed in the Agreement and applicable policies.

12. Legal Requirements

12.1 Service Provider may be required by law to provide access to Personal Information, such as to comply with a subpoena or other legal process, or to respond to government requests, including public and government authorities for national security and/or law enforcement purposes.

12.2 Service Provider will promptly inform You of requests to provide access to Personal Information and use reasonable efforts to redirect the authority that made the request to You, unless otherwise required by law.

12.3 To the extent Service Provider is required to respond to the request, it will first assess on a case-by-case basis whether the request is legally valid and binding on Service Provider, including whether the request is consistent with Applicable Data Protection Law. Any request that is not legally valid and binding on Service Provider will be resisted in accordance with applicable law.

13. Data Protection Officer

13.1 Service Provider has appointed a Chief Privacy Officer and a local Data Protection Officer. Further details on how to contact Service Provider's Chief Privacy Officer and, where applicable, the local Data Protection Officer, are available at https://www.alphametricx.com/privacy-policy.

13.2 If You have appointed a Data Protection Officer, You may request Service Provider to include the contact details of Your Data Protection Officer in the relevant Services order.

Exhibit B
Privacy Policy

1. INTRODUCTION

This privacy policy applies to the platform known as Alphametricx (https://alphametricx.com) ("Alphametricx Website"), associated subdomains, and any related online services ("Platform") operated by Infovision, Inc., a Texas corporation. The privacy policy outlines the manner in which Infovision collects, processes, stores, and protects personal information about individuals who interact with the Platform (the "Privacy Policy"). By using the Services or subscribing to the Platform, you ("You" or "Your") agree to the practices described in this Privacy Policy.
InfoVision, may act as a Data Controller, Data Processor, or Subprocessor depending on the specific services and context in which personal data is being handled. The role of InfoVision in each instance will be determined based on the nature of the interaction and in accordance with applicable data protection laws.

Definitions

"**Personal Data**" Refers to any information relating to an identified or identifiable individual. This includes:

- Obvious identifiers such as first name, last name, corporate email ID, phone number, company name, job title, and registered email address and password.
- Information collected automatically, such as IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views, and website navigation paths.
- Any other personal data voluntarily provided by the user.

"**Sensitive Personal Data**" Includes specific categories of data that may require explicit consent for processing, such as data revealing religious beliefs, political opinions, health data, genetic or biometric information, or other data deemed sensitive under applicable laws.

"**Processing**" Any operation or set of operations performed on personal data, including collection, storage, use, sharing, or deletion.

"**Cookies**" Small data files sent from a website and stored on a user's computer by their web browser while browsing. Cookies can enhance website efficiency and user experience.

"**Consent**" The explicit and informed agreement by an individual to the processing of their personal data for specific purposes.

"**Data Controller**" Refers to InfoVision, Inc., responsible for determining the purposes and means of processing personal data.
"**Data Subject**" Any individual whose personal data is processed by or on behalf of InfoVision, Inc.

"**Data Protection Authority**" The regulatory body in a specific jurisdiction tasked with enforcing applicable data protection laws and handling complaints regarding personal data processing.

"**Legitimate Interests**" The lawful basis for processing personal data when it is necessary for the organization's legitimate business purposes, provided these do not override the rights and freedoms of the data subject.

"**Retention Period**" The period during which personal data is stored, determined by the purposes of processing, legal requirements, or business needs.

"**International Data Transfer**" The transfer of personal data to a country outside the jurisdiction of the data subject, subject to compliance with applicable data protection laws.

"**Data Portability**" The right of a data subject to receive their personal data in a structured, commonly used, and machine-readable format and to transfer it to another organization.

"**Automated Decision-Making and Profiling**" Decisions made solely by automated means, including profiling, that produce legal effects concerning the individual or significantly affect them.

"**Privacy Team**" The designated team within InfoVision, Inc. responsible for handling privacy-related inquiries and managing personal data in compliance with this Privacy Policy.

2. PURPOSE AND USE OF PERSONAL DATA COLLECTED

- InfoVision will only use the personal data described above for the following purposes:
- To cater to Your request for the demo and manage Your account securely from any impersonation.
- Protect Your account from any malicious attacks – impersonation, identity and data theft.
- Administer and manage Alphametricx Website using web analytics.
- Personalize Alphametricx website for better use by You.
- Handling the enquiries or any topic of Your interest as requested by You.
- Keep Alphametricx Website secure and available for You to use.
- Publishing of Your personal data will only be in accordance with Your consent and/or were permitted by law.

If any kind of processing is based on Your consent, Infovision hereby inform You that You have the right to withdraw your consent at any time, without affecting the lawfulness of data processing based on consent before its withdrawal.

3. LEGAL BASIS FOR PROCESSING PERSONAL DATA COLLECTED

When You visit Alphametricx Website, the basis of processing Your personal data is to pursue Infovision legitimate interests in improving Alphametricx Website for better use.
When You request Infovision with any information, the basis of processing Your personal data is to take steps (respond) on Your request and in case if we process any sensitive personal data, Infovision processing will be based on Your prior explicit consent. In addition, InfoVision's role as Data Controller, Processor, or Subprocessor may vary based on the nature of data processing and the services. This role will be determined per applicable laws and in case, explicitly stated in relevant documents.

InfoVision do not believe our site is appealing to children, nor it is directed to children. Infovision do not knowingly collect personal data from children. If you are a parent of a child below certain age as defined by the applicable laws in individual's country, and you believe that, Your child has provided us with information about him or herself, please contact us (see 'Contact Us' section at the end of the page).

4. RETENTION OF PERSONAL DATA

Infovision will store Your personal data till the purposes for which Infovision process them (Infovision refer to the purposes as listed above in this policy) are met, or where Infovision is legally obliged to do so by the law, or where this is necessary for defending Infovision's interests in the context of judicial proceedings, or establish, exercise or defend Infovision's legal rights. Now since these needs can vary for different data types and purposes, the actual retention period may vary significantly and shall be in accordance with the applicable laws.

5. SECURITY OF PERSONAL DATA

Infovision will implement the necessary administrative, technical and organizational measures for ensuring a level of security appropriate to the specific risks that Infovision have identified. Infovision protect Your personal data against destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed. No method of transmission over the Internet, or method of electronic storage, is 100% secure, however, therefore, while Infovision strive to use commercially acceptable means to protect Your personal data, Infovision cannot guarantee its absolute security. At the same time, Infovision encourage You to use caution

when disclosing personal data online. More specifically, Infovision have taken the measures to protect Your personal data on our secure servers – restricted access, firewall protected and other measures as per the risks identified. If You have any questions about security on Infovision's website, please contact us (see 'Contact Us' section at the end of the page) and will be more than happy to respond / clarify your queries.

6. DISCLOSING PERSONAL DATA

Infovision may disclose your personal data to Infovision's employees, subsidiaries, vendors, affiliates, as necessary to fulfil the purposes mentioned above in this policy. But while sharing Your personal data to the vendors, Infovision will ensure that reasonable organizational and technical measures are in place at the vendor's place to safeguard Your personal data. Infovision may also disclose Your personal data where Infovision is legally obliged to do so by the law, or where this is necessary for defending Infovision's interests in the context of judicial proceedings, or to establish, exercise or defend Infovision's legal rights. Infovision may also transfer personal data in the event of the sale or transfer of all or any part of Infovision's business.

7. INTERNATIONAL TRANSFER OF PERSONAL DATA

Infovision may store, process and transfer the personal data within any of the countries in which Infovision operate to fulfil the purposes as mentioned above in this policy. Infovision's Privacy policy and the practices are designed to provide consistent level of protection to the personal data across Infovision's offices globally. In case of Your personal data being shared with Infovision's vendors based out in the countries where Infovision operate, Infovision will ensure that reasonable organizational and technical measures are in place at the vendor's place to safeguard Your personal data in accordance with the applicable data protection laws.

8. LINKS TO OTHER WEBSITES

In addition to the links to the websites hosted by Infovision, Infovision may include hyperlinks to, and details of, third parties' websites, which also includes pages or channels providing information about Infovision's organization on the social media websites – Instagram, X and LinkedIn. Please be aware that Infovision is not responsible for the privacy practices of such other sites. Infovision encourage You to be aware when You leave Alphametricx Website and to read the privacy statements of each website that collects personal data.

9. COOKIES WE USE

Cookie is a small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing. These cookies can be used to make your website

experience more efficient. These cookies are stored only on your device if they are necessary for the operation of the website. For more details on how, when and why cookies are used on our website and how Infovision manage them, please refer Infovision's Cookie Policy – https://alphametricx.com/cookies-policy

10. YOUR PRIVACY RIGHTS

In accordance to the applicable data protection laws, You have the right to:

- receive additional information regarding the processing of Your personal data;
- rectify Your personal data if it is incorrect;
- in certain cases, to have the erasure of Your some or all personal data;
- in certain cases, and on grounds relating to Your situation, to object to (part of) the processing of Your personal data;
- in certain cases, to restrict of or (part of) the processing of Your personal data; and
- data portability (receive your personal data in a structured, commonly used and machine-readable format and to (have) transmit(ted) your personal data to another organization)
- to lodge a complaint to the local data protection authority
- in certain cases, not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you.

11. CHANGES TO THIS PRIVACY POLICY

Infovision encourage You to carefully read this Privacy Policy. From time to time, Infovision may need to update this Privacy Policy. This may be necessary, for example, if the law changes or if Infovision changes its business in a way that affects the way Infovision process Your personal data. If this Privacy Policy will materially and/or substantially change, Infovision will actively inform You of this change at Infovision's website, or by email or by other communication means.

12. COMPLAINTS

You have the right to lodge a complaint at any time to the data protection authority in the country where You usually reside, Your country of work or country of infringement. At the same time, Infovision assure You that complaints shall be attended in the prescribed time frame, without impacting Infovision's quality of service or any discrimination to You as per the applicable data protection laws. However, Infovision would appreciate the chance to deal with Your concerns before You approach the data protection authority, so please contact us (see 'Contact Us' section at the end of the page) in the first instance.

CONTACT US

If You have questions about this Privacy Policy or Infovision's handling of Your personal data or want to exercise Your data rights, please contact Infovision's Privacy Team at privacy@alphametricx.com or write to the following address:

InfoVision, Inc.
Attention: Rajesh Kari
800 E Campbell Rd, Suite 388
Richardson, Texas – USA – 75081

Exhibit C
Cookie Policy

This Cookies Policy explains how InfoVision, Inc. ("we," "our," "us") uses cookies and similar technologies to recognize you when you visit our Platform or other services via https:/alphametricx.com (collectively, "Services"). It outlines what cookies are, the types of cookies we use, why we use them, how you can manage them, and your rights regarding them under US and EU laws.

1. What Are Cookies?

Cookies are small text files placed on your device when you access or interact with our Services. Cookies help us recognize your preferences, improve functionality, ensure security, and gather essential data about your usage of the platform. They also allow us to show personalized content, advertising, and conduct analytics to improve user experience.

In addition to cookies, we may use similar tracking technologies such as web beacons, pixels, and JavaScript, which help us collect information about your device and activity on our Platform.

2. Types of Cookies We Use

2.1. Essential Cookies

Essential cookies are necessary for the core functionality of the platform and ensure proper navigation and accessibility. These cookies are crucial to allow you to use the basic features of the Platform, such as logging in, saving progress, and ensuring secure browsing. Without these cookies, the Platform may not function optimally.

Examples:

- **Session Cookies**: These cookies maintain your session while navigating the Platform. They store temporary information, like your login credentials, to make sure you stay logged in during your session.
- **Security Cookies**: These cookies are used to verify that it is you who is making a request (for example, logging in or conducting a transaction) and to protect your account from unauthorized access.

Retention Period:

- Session cookies are stored only temporarily and expire once the session ends (usually when you close your browser).
- Security cookies may last up to 1 year to ensure secure authentication during that period.

2.2. Performance and Analytics Cookies

Performance cookies collect information about how visitors use our Services. These cookies allow us to monitor website performance, identify areas for improvement, and provide aggregated statistics on visitor behavior, such as the number of users visiting a particular page, click rates, session duration, etc.

- **Examples:**

  - **Google Analytics**: These cookies track website usage statistics to help us improve user experience by understanding user behavior, like how often users visit the site or which pages are most commonly accessed.

  - **Mixpanel**: Helps us analyze user interactions with the platform and gather insights for product improvements (for example, feature usage tracking).

- **Retention Period**:

  - **Google Analytics** cookies are retained for a maximum of 2 years for analytics purposes, after which they expire automatically.

  - **Mixpanel** cookies typically last for 13 months before being automatically cleared, unless you delete them earlier.

2.3. Functionality Cookies

Functionality cookies are used to remember your preferences (such as language settings, region, or customized themes) to provide a personalized browsing experience. These cookies improve the usability and personalization of the platform, allowing the site to remember your choices and enhance the user experience based on your preferences.

- **Examples**:

  - **Language Preference Cookies**: These cookies store your preferred language to ensure that your browsing experience is in the correct language without needing to select it repeatedly.

- **Theme Selection Cookies**: If our platform offers themes (light/dark mode), functionality cookies will remember your selection so that the theme persists across pages and sessions.

- **Retention Period**:

- These cookies persist between sessions and may remain on your device for up to 1 year before being cleared.

2.4. Advertising and Targeting Cookies

These cookies are used to deliver targeted advertisements to you both within and outside the Platform based on your browsing activity. They track your behavior across different websites and online platforms to display ads that are more relevant to you.

- **Examples**:

- **Google Ads**: Uses cookies to show you personalized ads based on your browsing history, search interests, or previous engagements with us, such as having visited the Platform.

- **Facebook Pixel**: Tracks your interactions with our platform and helps us deliver personalized advertisements through Facebook, Instagram, and other related ad networks.

- **Retention Period**:
- **Google Ads** cookies typically last between 30 days to 1 year depending on the campaign settings and user interactions.

- **Facebook Pixel** cookies have a lifespan of up to 90 days, depending on how often users visit the Platform.

2.5. Third-Party Cookies

We use third-party cookies from external services to provide additional functionalities, such as social sharing tools, embedded video content, or user authentication. These parties may use the information collected through their cookies for their purposes, which could include behavioral tracking or analytics.

- **Examples**:

- **LinkedIn**: To allow users to share content across social media or log in with their LinkedIn credentials.

- **Twitter**: Used for embedding Twitter feeds or enabling social interactions via Twitter, and may place cookies on users' devices.

- **Retention Period**:

  - These cookies generally remain on your device for up to 24 months, depending on the third-party service.

    For specifics on retention periods, please refer to the respective privacy policy of the third party.

3. Legal Basis for Using Cookies (EU Compliance)

Under the General Data Protection Regulation (GDPR), we are required to obtain your consent for the use of non-essential cookies, such as performance, functionality, and advertising cookies.

- Essential Cookies do not require consent as they are crucial for the functioning of the Services.

- For non-essential cookies, we ask for your explicit consent before they are placed on your device, which you can grant or withdraw at any time.

For our US users (especially those in California), under the California Consumer Privacy Act (CCPA):

- You have the right to opt-out of certain types of data collection conducted via cookies, including the "sale" of personal data, such as sharing data with advertisers for targeting purposes.

4. How We Obtain Your Consent

When you visit our platform, a cookie banner will appear, explaining the cookies used and giving you the option to accept all, decline non-essential cookies, or manage your preferences using our cookie management panel.

For EU users, we provide an intuitive mechanism to change your preferences at any time.

5. How to Manage and Delete Cookies

You can manage and delete cookies via your browser settings:

- **Google Chrome**: Click here
- **Mozilla Firefox**: Click here
- **Apple Safari**: Click here
- **Microsoft Edge**: Click here

Additionally, you can change your cookie settings directly on the platform by visiting the cookie preferences section.

6. Third-Party Tracking Technologies

We may allow third parties such as advertisers, social media platforms, or service providers to use cookies and tracking technologies on our Platform. Please be aware that these cookies are subject to the third-party's own privacy policies.

For example:

- **Google Analytics**: Privacy Policy
- **Facebook Ads**: Privacy Policy
- **LinkedIn**: Privacy Policy

7. Data Retention Periods

The cookies we use have varying retention periods, ranging from session-based cookies that expire once your session ends to persistent cookies that stay on your device for varying periods, such as 30 days to 2 years.

Please note that you can remove or delete cookies manually through your browser at any time. For more details, refer to our cookie management tools or your browser settings.

8. Updates to This Policy

This Cookies Policy may be updated periodically to comply with legal regulations and enhance user experience. Any changes will be posted on this page, and we will notify users in a prominent manner when significant updates are made.

The most recent update will always be marked at the top of the policy.

9. Your Rights Under CCPA and GDPR

California (US)

Under the CCPA, California residents have rights regarding their personal data:

- Right to opt-out of the "sale" of data.
- Right to request details on the data collected through cookies.
- Right to delete personal data upon request.

EU GDPR

For EU residents:

- Right to withdraw consent for the use of non-essential cookies.
- Right to access, rectify, or delete personal data stored via cookies.

10. Contact Us

If you have any questions or concerns about our Cookies Policy, please contact us:

InfoVision, Inc.
Email: privacy@alphametricx.com
Phone: (469)-619-3080
Website: https://www.alphametricx.com

By continuing to use our Services, you accept and consent to the use of cookies as described in this policy.

Exhibit D
Digital Assets Terms and Conditions

1. Introduction

These Terms and Conditions ("Terms") outline the rules and guidelines that govern your access to and use of both the **website** (referred to as the "Website") located at https://infovision.com & https://alphametricx.com and the **platform** known as AlphaMetricx (referred to as the "Platform"), together with any additional services and functionalities provided via these digital properties. The Website and Platform collectively represent online services or software tools made available by Service Provider to Users for business and professional use.

By accessing, browsing, or using the Website or Platform, you acknowledge that you have read, understood, and agree to abide by these Terms. Your use of the Website or Platform constitutes your express acceptance of these Terms, and any activities conducted on the Platform must adhere to all of the provisions outlined herein.

If you do not agree to the provisions specified in these Terms, you are prohibited from using the Website or Platform. In such cases, you must immediately cease accessing or using the Website and Platform. It is your responsibility to review these Terms regularly, as Service Provider may update, revise, or modify them at its sole discretion. Any continued use of the Website or Platform after any modifications to the Terms will constitute your acceptance of those changes.

In addition to these Terms, when using certain services or features available through the Website or Platform, you may be subject to additional terms, guidelines, policies, or agreements specific to those features or services. By accessing or using those features, you agree to comply with and be bound by those supplementary terms and conditions as well. These supplementary terms will be provided to you in advance of the relevant services, and if they conflict with these Terms, the supplementary terms will take precedence with regard to your use of those services.

The Website and Platform are made available for authorized business use, meaning that only individuals or organizations duly authorized to access these services for professional or commercial purposes should engage with the tools, content, and functions available on the Website and Platform. Personal or consumer use of the Website and Platform is strictly prohibited unless explicitly permitted.

If you represent an organization or business entity, by using the Website or Platform, you confirm that you have the necessary authority to agree to and bind your organization to these Terms.

2. Definitions

For the purpose of these Terms and Conditions, the following definitions apply in line with the other agreements or policies:

2.1 Website:

The term "Website" refers to https://alphametricx.com & https://infovision.com, which is the official website operated by Service Provider. This includes all webpages, sections, features, content, or resources available at https://alphametricx.com & https://infovision.com, as well as any related online services or additional content that may be offered. The Website encompasses all interactive elements such as blogs, articles, and public-facing pages, as well as user portals and back-end functionalities provided for registered users or authorized access. Essentially, the Website serves as the online front-end for accessing the services provided by Service Provider.

2.2 Platform:

"Platform" refers to AlphaMetricx, the software tool or service offered by Service Provider. The Platform includes all applications, functions, technologies, and systems that collectively allow businesses to interact with the service, access provided tools, and utilize the features designed to meet business needs. This definition extends to any features within the Platform such as dashboards, analytics tools, user management systems, integration points with other tools, and other online services that are built around AlphaMetricx. These services might include, but are not limited to, cloud-based applications, API integrations, and specialized software developed to enhance the business experience of using the platform. Additionally, "Platform" includes any future versions, updates, or enhancements of AlphaMetricx.

2.3 Users:

"Users" refers to any individual or organization that has authorized access to and interacts with the Website or Platform. This can be a company, corporation, or any other type of business entity and includes their employees, contractors, agents, or representatives who have been granted access under the terms set by Service Provider. Users may be responsible for managing multiple sub-accounts or teams that interact with the Platform on their behalf. By registering for and using the Website and Platform, Users agree to abide by all applicable policies, as defined in these Terms.

2.4 Customer Data:

“Customer Data” is any information or material, whether provided by the User or created through the use of the Website or Platform. Customer Data may include, but is not limited to, personal data (such as names, addresses, emails), textual data, multimedia content such as images, audio, videos, documents, metadata, analytics, and other proprietary materials shared or created during the use of the service. It is essential to note that Users retain ownership of Customer Data, but Service Provider is granted permission to process, store, and transmit it to provide necessary services under the Terms. Additionally, users must ensure they have obtained any necessary consents or rights to upload such data.

2.5 Services:

“Services” encompasses all the online functionalities and support that Service Provider provides through both the Website and Platform. This includes all the tools, applications, customer support, user assistance, and integrations made available for use by the Platform, such as customer support services, reporting, user guidance, API services, and system updates. These Services are designed to provide value to the Users by enabling them to perform specific tasks and operations that the Platform and Website support. The Services also extend to any specialized technical support, training resources, or consultancy services provided to users to ensure effective use of the Platform’s functionalities.

2.6 Third-Party Applications:

“Third-Party Applications” refers to any external software, services, or applications that are made available by parties other than Service Provider. These third-party tools might be integrated with or used in conjunction with the Website or Platform to offer additional functionality, enhance user experience, or provide external data that may benefit users. For example, external applications for email marketing, social media analytics, or customer relationship management (CRM) might interact with AlphaMetricx. Third-Party Applications may be subject to their own separate terms and conditions, which are outside of Service Provider's direct control. As such, the use of such third-party software and applications is governed by the specific terms agreed to with the third-party provider.

2.7 Service Provider:

“Service Provider” is the company that owns and operates both the Website and Platform. Service Provider is responsible for managing the infrastructure, business operations, compliance, user support, service development, and the ongoing evolution of the Website and Platform. This includes legal responsibilities, such as ensuring adherence to data protection laws, maintaining the integrity of user data, and managing agreements and licensing related to the use of the Website and Platform. Service Provider also oversees the terms under which the Platform is offered, including all conditions for the Services it provides and user access. Service Provider has the

exclusive right to modify, discontinue, or change elements of the Website and Platform as it sees fit.

3. Acceptance of Terms

By registering an account or using the Website or Platform, you represent and warrant that you are at least 18 years old, accessing the Services for business purposes, and have been granted authorization by Service Provider or its business partners. If accessing on behalf of an organization, references to "you" include your organization.

The Platform is intended for business entities and their authorized representatives only. By using the Platform, you represent that your business and its representatives comply with all applicable laws and regulations. Unauthorized use for non-business purposes may result in the suspension or termination of access and may violate these Terms.

4. Access and Use of the Platform

Service Provider grants a limited, non-exclusive, non-transferable, non-sublicensable, revocable license to use the Platform for authorized business purposes only. Unauthorized, unlawful, or non-business use is strictly prohibited. Users agree to promptly notify Service Provider of any unauthorized access or use.

By using the Platform, you agree to receive communications from the Company regarding updates, changes, or marketing materials. These notifications can be sent via email, push notifications, or through the Platform.

5. User Obligations

As a user of Service Provider’s Website or Platform, you are expected to fulfill certain responsibilities to ensure proper use of the services. These obligations are designed to promote a secure, lawful, and effective experience. Below is an elaboration of the different aspects of user obligations:

5.1 Account Information

5.1.1 Accurate Registration Information:

When creating an account, users must provide accurate, current, and complete information. This is vital for ensuring smooth functionality, user support, and security within the Platform. The details provided during registration—such as names, contact information, business identification, and any relevant verification data—must reflect the truth and the current state of the user or business entity.

5.1.2 Notification of Changes:

It is the user's responsibility to promptly notify Service Provider of any changes to the account information. This may include updates to contact information, business details, or roles within the organization that affect user access to the Platform. Maintaining accurate information ensures that communications from Service Provider—such as service updates or security notices—reach the correct recipient in a timely manner.

5.1.3 Confidentiality of Credentials:

Users are solely responsible for safeguarding their account credentials, such as passwords and access codes. These login details should not be shared, transferred, or disclosed to unauthorized individuals. Service Provider cannot be held liable for any breach of security or misuse of the Platform resulting from the unauthorized sharing or improper handling of account credentials.

5.2 Acceptable Use

5.2.1 Prohibited Activities: Users are strictly prohibited from engaging in activities that breach applicable laws or regulations. This includes, but is not limited to:

Transmission of Harmful Content: Users must refrain from posting, sending, or otherwise transmitting any content that could be deemed offensive, abusive, defamatory, or illegal. This can include discriminatory materials, harassing messages, or explicit content that violates laws on decency, privacy, or online conduct.

Promoting Harm or Violence: The Platform must not be used to promote any harmful activities, such as violence, hatred, illegal behavior, or actions that can result in harm to individuals, communities, or society.

5.2.2 Unauthorized Access and System Integrity: Users are prohibited from taking any action that could disrupt, damage, or gain unauthorized access to the Platform's systems or data. This includes, but is not limited to:

- **Unauthorized Access:** Users must not attempt to access areas of the Website or Platform that they are not authorized to use.
- **Reverse Engineering:** Attempting to reverse-engineer, decompile, disassemble, or tamper with the Platform's code or software in any way is explicitly prohibited. These actions could compromise system security, the functionality of the service, or the privacy of other users.
- **Harmful Actions:** Engaging in activities designed to circumvent security protocols or degrade service quality (such as introducing malware or spamming the system) can lead to account suspension or legal action.

5.3 Data Security

5.3.1 Reasonable Security Measures:

Users are responsible for implementing security measures to protect both their personal account and associated devices used to access the Platform. This could involve setting strong, unique passwords, employing encryption on stored data, and using device protection tools such as firewalls or antivirus programs. Users must take responsibility for actions that could expose data to cyber threats, ensuring a safe browsing and usage environment.

5.3.2 Notification of Unauthorized Access or Breaches:

If a User suspects any unauthorized access to their account, device, or data (e.g., hacking, phishing attacks, or an attempted data breach), they must immediately report the incident to Service Provider. This prompt notification enables Service Provider to initiate corrective actions, such as suspending the account or securing data, and ensuring no further damage occurs. Users should stay vigilant for any suspicious activity involving their account.

5.4 Legal Compliance

5.4.1 Compliance with Applicable Laws:

Users agree to abide by all local, state, national, and international laws and regulations applicable to the use of the Website or Platform. This includes a variety of legal obligations that can affect how users interact with and utilize the services. Some of the most relevant legal areas include:

- **Data Protection and Privacy Laws:** Compliance with laws such as the General Data Protection Regulation (GDPR) in Europe, California Consumer Privacy Act (CCPA) in California, and other regional or local regulations concerning the processing, storage, and management of personal data.
- **Intellectual Property (IP) Laws:** Users must respect intellectual property rights, including copyrights, trademarks, patents, and other proprietary rights. This means that Users must refrain from using, distributing, or reproducing content (such as software, articles, or digital media) that infringes upon third-party IP rights. This also extends to respect for proprietary software and code developed by Service Provider.
- **Other Relevant Regulations:** In addition to data protection and IP laws, there may be other regulations regarding business operations, cybersecurity, and e-commerce standards that Users must adhere to while using the services offered on the Website or Platform.

Users must actively ensure that all content uploaded or shared through the Website or Platform complies with legal obligations, especially concerning privacy and IP laws. Failing to do so may expose users to legal liabilities and the potential suspension or termination of access to the services

provided by Service Provider. Service Provider reserves the right to intervene if it becomes aware of any activities by Users that contravene these legal guidelines, including enforcement of appropriate actions such as account suspension or referral to legal authorities.

6. Customer Data

The management, handling, and protection of customer data is essential when using the Website and Platform. The following provisions explain the ownership, responsibilities, restrictions, and data management related to customer data.

6.1 Ownership and Responsibility

6.1.1 Ownership Retained by Users:

Users maintain full ownership of all Customer Data they provide while using the Website or Platform. “Customer Data” includes all types of data submitted to or stored in the Platform—whether it is personal, business-related, or any other data uploaded by users (e.g., text, images, audio, video, files, etc.). This means that even though Service Provider processes and stores this data for operational purposes, Users remain the rightful owners of their own data.

6.1.2 Limited License for Service Provider to Process Data:

In order to provide users with the necessary services, Users grant Service Provider a limited license to process, store, and transmit their Customer Data. This license is specific to the operation of the Platform and the delivery of the Services. This means that:

- Service Provider can use, store, and manage the Customer Data strictly for the purpose of providing services, such as data analysis, system maintenance, user support, and any other activity directly related to fulfilling Service Provider's obligations.
- Service Provider cannot use the data for any other purpose outside these agreed-upon service functions.
- Service Provider will handle Customer Data in accordance with applicable data privacy laws and its privacy policies. However, it is important to note that Users maintain control and ownership of the data and Service Provider only receives permission to handle it for service-related purposes.

6.2 Prohibited Content

6.2.1 Sensitive Personal Data and Authorization Requirements:

Users are prohibited from uploading certain categories of sensitive personal data unless they have explicit and proper authorization. This includes sensitive information such as:

- **Health Data:** Medical records, personal health information, or any data that falls under specific regulations such as HIPAA (Health Insurance Portability and Accountability Act).
- **Data about Minors:** Any data related to minors that is restricted or regulated by child protection laws or privacy regulations must not be uploaded without explicit authorization, as required by law.
- **Sensitive Personal Information:** Other sensitive data categories could include financial records, personal identification numbers (such as social security numbers or national identity numbers), or biometric data.

Important: If users plan to upload any such sensitive data, they must ensure they have received proper consents from individuals concerned and that they adhere to relevant regulations or legal frameworks (e.g., GDPR, CCPA, or other local privacy laws). Any misuse of sensitive data without authorization can result in significant legal consequences.

6.2.2 Harmful or Malicious Content:

Users are also prohibited from uploading or sharing any harmful content that could compromise the functionality of the Website or Platform. Specifically:

- **Malicious Software and Viruses:** Users must not upload or distribute software, viruses, malware, ransomware, spyware, or any harmful code that could damage, disable, or disrupt the operations of Service Provider's systems or any third-party system.
- **Intellectual Property Violations:** Users must not upload content that infringes upon intellectual property (IP) rights, such as copyrighted materials, trademarks, patents, or proprietary information owned by others. Violating IP rights could expose the user to lawsuits, legal action, and penalties.

Service Provider takes content moderation and intellectual property compliance seriously. Violations of these rules may lead to suspending or terminating the User's access to the Platform, as well as legal action in extreme cases.

6.3 Data Backup

6.3.1 Service Provider's Liability on Data Backup:

While Service Provider is committed to maintaining the security and availability of Customer Data stored within the Platform, it is important to note that Service Provider is not responsible for backing up Customer Data. In the event of data loss, whether through technical issues or unforeseen circumstances, Service Provider cannot guarantee that lost data will be recoverable unless specific backup solutions or data protection measures are provided for in a separate agreement.

6.3.2 User Responsibility for Data Backups:

Users are strongly encouraged to maintain their own backups of critical data stored within the Platform. Backup copies can be stored securely on third-party platforms or local storage systems for additional protection. Doing so helps ensure that data loss does not impact business operations or important records in the event of unexpected downtime, data corruption, or any other issue related to data security or platform functionality.

If Customer Data is crucial for business operations, users should adopt a regular backup strategy and consult Service Provider for any available services or solutions that may assist with data backup needs.

7. Intellectual Property

The terms related to intellectual property (IP) ensure that the ownership and use of materials, assets, and content between Service Provider and Users are clearly defined. This section highlights both the ownership rights Service Provider holds and how user feedback or contributions may be handled.

7.1 Service Provider Rights

7.1.1 Ownership of Website, Platform, and Services:

Service Provider retains full ownership of all intellectual property rights related to the Website (https://alphametricx.com & https://infovision.com), the Platform (AlphaMetricx), and any related Services it provides. This includes, but is not limited to, the following:

- **Proprietary Software:** All software used within or developed for the Platform is considered the intellectual property of Service Provider. This software could include any applications, programs, databases, and systems that power the Website or Platform's functionality.
- **Trademarks and Logos:** Service Provider owns and controls all trademarks, logos, brand names, and identifiers associated with the Website and Platform. This includes any registered trademarks (e.g., Service Provider's brand name or AlphaMetricx) or unregistered marks (e.g., logos, visual designs, and symbols associated with the services).
- **Other Proprietary Rights:** This also extends to any trade secrets, methods, content, system designs, algorithms, and unique technologies developed and used by Service Provider in connection with providing the services on the Website or Platform.

These intellectual property elements are protected by intellectual property laws, such as copyrights, patents, trademarks, and trade secret laws, as applicable. Users acknowledge that by accessing and using the Website and Platform, they do not gain any ownership of Service Provider's intellectual property and that all such rights remain exclusively with Service Provider.

7.1.2 License to Use the Services:

Service Provider grants Users a limited, non-transferable, revocable license to use the Website, Platform, and related Services. This license is given solely for the intended purpose of the service provided and only for lawful business or organizational purposes, as outlined in these Terms and Conditions. The specific details of the intended use include using the Platform for legitimate business operations that comply with the Terms of the Agreement.

Important limitations of the license:

- The license cannot be transferred to third parties, sold, or sublicensed.
- The license is revocable, meaning Service Provider has the right to withdraw this license if the user violates any terms or conditions.
- The use is restricted to the original intended purpose; Users cannot reverse-engineer, modify, or repurpose Service Provider's IP, software, or other protected materials for other uses outside of what is permitted in the Terms.

7.2 User Contributions and Feedback

7.2.1 Use of User Feedback and Suggestions:

Service Provider encourages users to provide feedback, suggestions, and ideas for improving the services, features, or usability of the Platform. However, Users must understand that any feedback or contributions provided by them are considered the property of Service Provider once submitted.

- **No Compensation for Feedback:**

When Users submit feedback or suggestions (e.g., ideas for platform improvements, feature enhancements, reports of issues, etc.), Service Provider is under no obligation to compensate the users. This means that Service Provider does not have to provide payment, royalties, or any other form of compensation for using or implementing ideas or suggestions shared by users, even if such ideas lead to valuable innovations.

- **Right to Use Feedback for Improvement:**

Service Provider is free to use any feedback or suggestions provided for its internal purposes, including to enhance the Website, Platform, and overall service offerings. This can involve adopting user feedback to improve functionality, fix bugs, create new features, or refine the overall user experience.

8. Third-Party Services

This section covers the interaction between the Service Provider Platform and services provided by third parties, including integrations, compliance, liability, and data usage. It ensures that users

are aware of the risks and responsibilities associated with using third-party services in connection with the Platform.

8.1 Integration with Third-Party Services

- **Platform's Integration with Third-Party Services or APIs:**

The Platform may allow integration with third-party services, applications, or APIs (Application Programming Interfaces). This means that the Platform can interconnect or interact with external services that may provide additional functionality or enhance the user experience. These third-party services can range from payment processors, marketing tools, analytics, communication services (such as email or messaging), or other business tools and software that complement the core features of the Platform.

Acknowledgment of Third-Party Terms:

Users acknowledge and agree that when they use any integrated third-party services, they will be subject to the respective third-party service providers' terms and conditions. These terms will govern the specific interactions between the user and the third-party service. Service Provider emphasizes that users must review and comply with these additional terms to ensure that they are fully informed about their rights and responsibilities when accessing and using third-party services.

Responsibility for Third-Party Services:

Service Provider makes it clear that it does not control or manage these third-party services, meaning that any use of these services is at the user's own risk. Service Provider is not responsible for ensuring the continuous availability or reliability of these third-party services, nor does it guarantee their accuracy in providing the services offered. If there are any issues, such as third-party services being down or having functional discrepancies, Service Provider will not be held liable or required to provide support for these issues.

8.2 Liability

- **Compliance with Laws and Third-Party Terms:**

Users are responsible for ensuring that their use of third-party services complies with applicable laws and regulations, as well as the specific terms of the third-party services. Since these third-party services often have their own rules and terms, it is essential for users to understand and abide by them.

Key Responsibilities of the User:

- Ensuring legal compliance when interacting with third-party services
- Reviewing and accepting the third-party terms before using the service
- Ensuring the Platform's usage, combined with third-party services, does not breach any contractual obligations, data protection laws, or intellectual property rights

Note: Service Provider disclaims responsibility for any consequences arising from a user's non-compliance with third-party terms or applicable laws when using integrated third-party services.

8.3 Data from Third Parties

- **Accuracy of Third-Party Data:**

Service Provider may source or use third-party data to enhance features, services, or insights within the Platform. For example, this could include market analytics, financial data, or other forms of information that may provide additional functionality to Platform features. However, it is important to understand that Service Provider does not guarantee the accuracy or completeness of data obtained from third parties.

Implications for the User:

- Service Provider will not be held liable for decisions made based on third-party data that may be inaccurate, outdated, incomplete, or misleading.
- Users should use their judgment when relying on any data provided through third-party integrations.

Users are encouraged to independently verify any third-party data they use for critical business decisions to ensure the reliability of such data.

8.4 Modifications

- **Service Provider's Right to Modify, Limit, or Discontinue Third-Party Services:** Service Provider reserves the **right** to make changes related to its use of third-party services. This means Service Provider has the discretion to:
  - Modify the level of service provided by third-party integrations or features,
  - Limit access to specific third-party services,
  - Discontinue third-party services or integrations at any time.

Notification of Changes:

While Service Provider will strive to provide notice of any changes, the discontinuation or limitation of third-party services may happen without prior notice due to various reasons (e.g., external vendor decision-making, regulatory changes, service performance issues). Users need to be aware of these potential changes and adjust their use of the Platform accordingly.

User's Obligation to Stay Informed:

Since third-party service changes are outside of Service Provider's control, it is ultimately the user's responsibility to monitor these integrations and ensure continued compatibility with their business needs. If access to a crucial third-party service is removed or altered, users may need to seek alternative solutions for that specific functionality.

9. Indemnity

9.1 User Agreement to Indemnify and Defend Service Provider

- **Indemnification Obligation:**

The user agrees to "indemnify" Service Provider, which means that they will protect and compensate Service Provider for any losses or damages if claims are made against the company in certain situations. Essentially, if someone sues or makes a claim against Service Provider due to the user's activities, the user will be required to handle the financial costs, damages, or penalties, even if Service Provider did not directly cause the issue.

- **Duty to Defend:**

The user also agrees to take on the responsibility to defend Service Provider in the event of a claim. This may involve covering the costs of legal defense if the company faces lawsuits or claims related to the user's actions. The user would need to engage legal counsel or take other necessary steps to manage the defense of Service Provider against such claims, provided it is reasonable.

- **Holding Harmless:**

The "hold harmless" clause requires users to ensure that Service Provider and related parties are not negatively impacted (or financially harmed) due to a legal situation that arises due to the user's actions or breach of the agreement. In practice, the user will bear the responsibility for costs like settlements, damages, and legal expenses.

9.2 Scope of Indemnity

9.2.1 Your Use of the Platform, Including Content You Upload:

- The user agrees to indemnify Service Provider for any claims or damages resulting from their use of the Platform. This includes all actions taken while using the Platform (whether using features, interacting with the software, or accessing services).

- **Content You Upload:** Users are solely responsible for all content they upload to the Platform, including text, images, video, code, or any other data. If the user uploads harmful, illegal,

defamatory, or infringing content, Service Provider will not be held liable; instead, the user will bear responsibility for addressing claims related to such content.

9.2.2 Violation of Laws or this Agreement:

- If the user violates any laws, regulations, or the terms of the agreement (whether consciously or negligently), they will need to compensate Service Provider for any damages that result from such violations.

- **Legal Violations:** This could be any breach of local, national, or international laws while using the Platform. For instance, violating data protection laws, fraud, cybercrime, or failing to follow specific platform rules can lead to indemnification responsibility.

9.2.3 Infringement of Third-Party Intellectual Property:

- If the user infringes on third-party intellectual property rights (e.g., using copyrighted content without permission or trademark violations), they agree to indemnify Service Provider against any claims or losses that may arise.

- This specifically includes instances where third parties assert ownership over content or materials the user has provided or uploaded that infringe upon patents, trademarks, copyrights, or other proprietary rights.

9.3 Service Provider's Right to Assume Exclusive Defense

Exclusive Defense of Indemnified Matters:

Service Provider reserves the right to take over the defense of any matter for which indemnity is required. In such cases, Service Provider would handle the legal proceedings, potentially with its own legal counsel, and decide how best to approach the case.

- **Reason for Exclusive Control:** Service Provider might choose to assume control of a claim to minimize its own liability and handle the defense in the most strategic way possible. This might include settlement negotiations or engaging in court proceedings.

- **User's Obligation to Assist:** While Service Provider has the discretion to handle the defense, users must still cooperate with Service Provider during the proceedings, providing relevant documents, information, or evidence related to the case.

9. Fees and Payment

9.1 Request for Platform Demonstration

- Users may request a demonstration of the Platform before deciding whether to subscribe. This option is typically offered to give potential subscribers the opportunity to explore the features, functionalities, and performance of the Platform.
  - **Purpose of Demonstration:** The demonstration allows users to evaluate if the Platform meets their needs, familiarize themselves with its services, and understand its interface before committing to a subscription.
  - **Terms of Demonstration:** The details of the demonstration, such as its duration and scope, are typically outlined during the request process or in a follow-up communication with Service Provider. It is expected that Users will engage with the Platform during this time to assess its relevance for their business.

Note: The demonstration is optional**,** and users are not required to proceed to a paid subscription unless they are satisfied with the Platform's offerings.

9.2 Payment of Annual Subscription Fee

- **Payment for Subscription:**

If users decide to subscribe to the Platform after the demonstration, they must pay an annual subscription fee as determined by Service Provider.

- **Subscription Agreement:** By subscribing, users agree to pay the applicable annual fee in exchange for continued access to the Platform and its services. The fee may vary depending on the scope of access or services requested.
- **Payment Methods:** Typically, the payment methods available could include traditional bank transfer (e.g., ACH or wire transfer) or other mutually agreed methods of payment. These details would be provided in the subscription agreement.

The specific fee amount and payment schedules are usually outlined during the onboarding process. Service Provider may require payment upfront for the full year to secure access.

- **Account Activation upon Payment:**

After payment of the subscription fee**,** Service Provider will activate the User's account**.** This means:

- Users will gain full access to the Platform's tools, features, or services as per the subscription plan they've selected.
- **Account Setup:** The user will typically be able to customize or configure their user account as needed.

Account activation generally occurs within a set period after payment receipt, ensuring the User can start using the Platform's features immediately once the transaction is processed.

9.3 Automatic Subscription Renewal

- The subscription to the Platform is set to automatically renew at the end of each subscription term unless canceled. The renewal ensures that users maintain continuous access to the Platform without interruption.
    - **Renewal Term:** The renewal is for an additional one-year term (unless otherwise specified) and is charged at the same subscription rate as the initial term unless stated otherwise by Service Provider.

Note: Automatic renewal aims to prevent any disruption in service. However, it is the User's responsibility to review their account regularly to ensure that the service aligns with their needs for each subsequent year.

9.4 Cancellation of Subscription

- **Cancellation Policy:**

Users are able to cancel their subscription if they no longer wish to continue accessing the Platform. However, users are required to notify Service Provider at least 60 days before the end of their subscription term.

- **Notice Requirement for Cancellation:** The notification of cancellation must be made in writing**,** which could mean through email or another agreed-upon communication channel. This written notice serves as a formal request to cancel the renewal process and prevent further charges from occurring.
- **Non-Cancelation Result:** If the subscription is not canceled within the required timeframe, the subscription will automatically renew for another year, and the user will be charged the subscription fee for that new term.

9.5 Non-Refundable Payments

- **Non-Refundability of Payments:**

Once the subscription payment is made, payments are non-refundable**.** This means:

- **No Refund upon Cancellation:** If a user cancels during a current subscription term, they will not receive a refund for any unused portion of the subscription period. The subscription is designed for an annual commitment, and fees are due upfront for the entire year.
- **No Pro-Rated Refunds:** If the User requests early cancellation, Service Provider will not issue pro-rated refunds for the portion of the year that was not used.

Note: It is important for users to review their commitment before subscribing, as once paid, the fee is final and non-refundable.

10. Suspension and Termination

10.1 Suspension of Access

Service Provider may suspend access to the Platform or its associated services under certain conditions. Suspension typically involves temporarily restricting a user's access to their account, tools, or features of the Platform. Suspension can happen without warning in certain serious cases, while other cases might involve a prior notice to the user.

Key reasons for suspension include:

1. **Violation of Terms**
    - **Failure to comply** with the Terms and Conditions: If the User engages in activities that breach the established terms or rules of behavior outlined in the Terms (e.g., engaging in illegal activities, misuse of intellectual property, or violating data protection policies).
    - **Use of Platform for malicious purposes**: If the user uploads or disseminates harmful content, such as malicious software or prohibited data, Service Provider may temporarily suspend access to protect the security and stability of its Platform.
    - **Unacceptable behavior**: If the user engages in conduct that damages Service Provider's reputation or the reputation of its users, like harassment, promoting violence, hate speech, or misleading advertising.
2. **Failure to Make Payments**
    - If the subscription fee is not paid by the due date, Service Provider may suspend access to the Platform until outstanding payments are cleared.
    - **Late Payments or Non-Payment**: If users fail to pay the required fees within the defined grace period (if applicable), Service Provider reserves the right to restrict access or lock accounts temporarily, preventing further use of the Platform or its services.
3. **Security Concerns**
    - **Suspicion of security risks**: If a user's account is suspected of being compromised—such as potential unauthorized access, system hacking, or if there are indications that the account or a connected device is being misused—Service Provider may suspend access to mitigate potential harm.
    - **Preventing data breaches or other vulnerabilities**: Service Provider will temporarily suspend an account if there are concerns about data security**,** hacking attempts, or other technological breaches that put the Platform, the user's account, or other users at risk.

During the suspension period, the user will typically not be able to access the Platform's functionalities (e.g., features, services, or applications), and may need to take corrective actions such as paying fees, removing prohibited content, or resolving security issues, depending on the cause of the suspension.

10.2 Termination of Account

Termination is a more permanent action than suspension and involves the complete deactivation or removal of a user's account and access to all related services. There are two types of termination in this context: termination by the user and termination by Service Provider.

Termination by the User

- **Voluntary Termination**: Users have the option to terminate their accounts at any time. However, termination requires prior written notice to Service Provider.
    - **Written Notice Requirement**: Users must provide Service Provider with an official notice (email or other written forms of communication) about their intent to cancel or end their subscription to the Platform.
    - **Account Deletion**: Upon receiving written notice, Service Provider will typically proceed with disabling the user's account and removing access to the Platform, though some services (such as technical support) may continue for a certain period, as applicable, depending on the subscription plan.
    - **Outstanding Fees or Data**: Depending on the contract, users may still be liable for any unpaid fees or obligations due before the cancellation, and their data may need to be processed per the data retention outlined elsewhere in the Terms. Users should clarify any post-termination considerations in the notice to Service Provider.

Termination by Service Provider

- **Voluntary Termination:** InfoVision reserves the right to terminate user accounts at its sole discretion under the following circumstances:

    - If InfoVision discontinues or makes significant modifications to the Platform or Services that affect the user's ability to continue using them.
    - If InfoVision determines that maintaining the user account is no longer commercially viable, either due to inactivity, changes in business strategy, or other operational reasons.
    - If InfoVision ceases operations or undergoes a merger, acquisition, or restructuring that impacts user accounts.
    - If required by law or regulatory directives to terminate certain accounts.
    - **Notice Period:** In the event of voluntary termination, InfoVision will provide the user with at least 30 days' written notice, except in cases where immediate termination is required by law or regulatory obligations.
    - **Termination Without Notice:** InfoVision may terminate a user's account without prior notice in the following cases; (i) If continued access to the Platform poses a security risk or threatens the integrity of InfoVision's systems, networks, or other users; (ii) If the user engages in fraudulent activities, unlawful conduct, or severe violations of the Terms and Conditions; (iii) If termination is mandated by a court order, regulatory action, or legal requirement that prohibits prior notice; (iv)If the user's subscription has expired, and no renewal or payment has been received within the specified grace period (if any).

- **Refunds & Data Access:** If InfoVision initiates voluntary termination, users may be eligible for a pro-rata refund of any prepaid but unused subscription fees, depending on the terms of their agreement. Users will also be given a reasonable period to retrieve their data before account closure, subject to InfoVision's data retention policies.

Termination for Violations of Terms:

Service Provider reserves the right to terminate user accounts if users violate key aspects of the Terms and Conditions or if the violations are severe or ongoing despite warnings. The types of violations that may lead to termination include, but are not limited to:

- **Repeated breach of the Acceptable Use Policy** (such as fraud, misuse of the Platform, or malicious activities like spreading harmful code).
- **Violation of payment obligations** if users fail to pay owed fees, especially after receiving multiple notices.
- **Unauthorized access or sharing of confidential information**, intellectual property theft, or instances where a user violates another's rights.
- **Infringement on data security and protection laws** that jeopardize other users or the platform itself.
- **30 Days' Notice:** Service Provider is typically required to provide 30 days' notice before terminating the user account. The notice period allows the user a chance to address the violation or disputes, allowing them time to correct the issue or resolve the problem.

Consequences of Termination

- **Loss of Access**: Upon termination**,** whether by the user or Service Provider, the user will lose all access to the Platform and its associated features or services.
- **Data Removal**: Service Provider will likely proceed with removing or archiving any user-provided data upon account termination, depending on the data retention policies.
- **No Refunds**: Termination does not entitle users to refunds for the remainder of their paid subscription or services. Payments are generally non-refundable, regardless of whether termination is voluntary or due to a breach.

11. Privacy and Data Protection

Service Provider processes and controls Customer Data and Author Data in compliance with GDPR, CCPA, and other data protection laws. Detailed practices are outlined in Service Provider's Privacy Policy and relevant agreements. Users must obtain necessary consents for data they upload.

12. Warranties and Disclaimers

12.1 Service Provider provides its services, including the Platform and associated services, on an "as-is" basis, meaning that these services are provided to users without any express or implied warranties. This includes, but is not limited to, any implied warranties of merchantability and fitness for a particular purpose**.** By using the Platform and its associated services, users acknowledge and agree that they do so at their own risk and that Service Provider makes no guarantee regarding the performance, reliability, or availability of the Platform.

12.2 Service Provider does not warrant or assure that the Platform, its services, or any associated content will meet the expectations or needs of users at all times. Users should be aware that the Platform may have limitations, technical bugs, or issues that could impact its performance. Additionally, the Platform may not always function optimally or as anticipated by the user, and it is possible that certain services may be unavailable or malfunction due to unforeseen technical issues, bugs, downtime, or scheduled maintenance.

12.3 Service Provider makes no representation that the Platform or its services will always be available without interruption or will always operate error-free**.** The availability of the Platform may be subject to external factors outside of Service Provider's control, such as third-party service interruptions, technical difficulties, or other unforeseen challenges. While Service Provider makes reasonable efforts to ensure the continuity and reliability of the Platform, it is not liable for any service failures, downtime, or disruptions.

12.4 Furthermore, Service Provider disclaims any implied warranties related to the Platform's fitness for a particular purpose or its merchantability. Service Provider does not guarantee that the Platform will be suitable for any specific business needs or user requirements. For example, even if a user relies on the Platform for certain tasks like data analysis, Service Provider does not guarantee that the Platform will consistently meet these business objectives or perform according to user expectations. Additionally, any analysis, insights, or recommendations generated by the Platform may not be accurate, complete, or reliable. The Service Provider disclaims any responsibility for business decisions made based on such outputs, and users assume full responsibility for any risks or consequences arising from their reliance on the Platform's data or insights.

12.5 As with any technology-based service, users understand that technical errors or glitches may arise. Service Provider does not assume responsibility for fixing or rectifying such issues unless explicitly agreed to by the parties. By using the Platform, users acknowledge that they are accepting the inherent risks involved in using a service that may experience disruptions, service failures, or technical limitations from time to time.

13. Limitation of Liability

Service Provider's liability to the user for any claims, damages, losses, or expenses arising out of or in connection with the use of the Website, Platform, or Services shall be limited to the total amount paid by the user for the Services in the 12 months immediately preceding the date of the claim**.** In no event shall Service Provider be liable for any indirect**,** incidental**,** special**,**

consequential**, or** punitive damages, including, but not limited to, loss of profits**,** business interruption**,** reputational harm, or loss of business opportunity**,** whether arising in contract, tort, or otherwise, even if Service Provider has been advised of the possibility of such damages.

By using the Website, Platform, or Services, the user acknowledges and agrees that this limitation of liability represents a fair allocation of risk between the parties and that the amount paid by the user for the Services is the agreed-upon measure of Service Provider's potential liability.

14. Governing Law and Dispute Resolution

14.1 These Terms and Conditions shall be governed by and construed in accordance with the laws of the State of Texas, United States of America, without regard to its conflict of law principles. By accessing or using the Website and Platform, you agree that any dispute, claim, or controversy arising out of or relating to these Terms, your use of the Platform or Website, or any services provided therein, shall be governed by the laws of Texas, USA.

14.2 In the event of any dispute or claim arising out of or relating to these Terms or your use of the Platform, you agree to make a good faith effort to resolve the issue informally and amicably. If such an attempt at informal resolution is unsuccessful, all disputes that cannot be resolved informally will be exclusively adjudicated in the competent courts of Texas. The courts located in Texas shall have sole and exclusive jurisdiction, and the parties waive any objection to venue in these courts.

15. Compliance with Global Standards

Service Provider is committed to complying with international regulations governing data protection and privacy, including but not limited to the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. These regulations set forth requirements for the collection, use, and protection of personal data, and Service Provider strives to meet these legal standards in all operations, ensuring that User data is handled responsibly and in compliance with the applicable laws.

However, it is important to note that Users are also responsible for ensuring that their use of the Platform and services complies with any local laws, regulations, or data protection requirements that may apply based on their specific geographic location, jurisdiction, or business operations. Users must take all necessary precautions to remain compliant with relevant legal obligations, such as obtaining appropriate consents for processing personal data, ensuring transparency in data collection practices, and protecting the privacy rights of individuals under applicable data privacy laws.

Service Provider reserves the right to modify, update, or alter its policies and practices to maintain compliance with new or evolving regulations, and Users should stay informed about any such changes that might affect their use of the Platform and the handling of Customer Data and Author Data.

16. Changes to Terms

Service Provider reserves the right to amend, modify, or update these Terms and Conditions at any time, at its sole discretion. Any changes to these Terms will be communicated to Users by posting the revised version on the Website or through direct notification via email, within the Platform, or through other means deemed appropriate by Service Provider.

In the event of significant amendments or updates that may impact User rights or obligations, Service Provider will notify Users in a reasonable and timely manner. Users are responsible for reviewing these Terms regularly to stay informed of any changes.

By continuing to access or use the Website, Platform, or Services following the posting of updated Terms, Users signify their acceptance of the revised Terms. If a User does not agree to the changes made, they must cease using the Website and Platform immediately. Failure to notify Service Provider of a disagreement with the updated Terms or continuing to use the Services shall be deemed as acceptance of the revised Terms.

17. Contact Information

For questions or concerns, please contact Service Provider at:

InfoVision, Inc.

Attention: Rajesh Kari

800 E Campbell Rd, Suite 388, Richardson, Texas -75081

contact@infovision.com

(469)-619-3080

EXHIBIT E

AI USAGE POLICY

Last Updated: *January 1, 2025*

AlphaMetricx, an AI-powered media intelligence platform ("Platform") by InfoVision, Inc. ("InfoVision"), is committed to using artificial intelligence (AI) responsibly, ethically, and in compliance with global regulatory frameworks. This AI Usage policy outlines the scope, limitations, and principles governing the use of AI technologies on the Platform ("Policy").

What is Artificial Intelligence (AI)?

Artificial Intelligence (AI) is a branch of computer science focused on creating systems capable of performing tasks typically requiring human intelligence. AI involves the development of algorithms and models that enable machines to learn from data, make decisions, and improve over time without explicit programming.

Key components of AI include:

- **Machine Learning (ML):** Algorithms that use data to train models for pattern recognition, prediction, and decision-making.
- **Natural Language Processing (NLP):** AI's ability to understand, interpret, and generate human language for tasks like sentiment analysis or text summarization.
- **Computer Vision:** The ability of AI systems to analyze and process visual data, such as images and videos.
- **Predictive Analytics:** Using historical data and AI models to forecast trends and behaviors.
- **Automation:** AI-driven tools to streamline repetitive tasks and enhance operational efficiency.

AI systems in the Platform are designed to process large datasets, derive insights, and provide actionable intelligence while adhering to principles of transparency, fairness, and ethical use.

Definition of Users/User

For the purposes of this Policy, "Users" "User" refers to any individual, group, or organization that interacts with or derives value from the Platform. Users are categorized into the following groups:

1. End Users:

- Individuals accessing the platform to obtain insights, analytics, and media intelligence for professional use.

2. Enterprise Clients:

- Businesses and organizations using the platform as part of their operations, strategy, or decision-making processes.
- Includes clients integrating the Platform outputs into workflows for media monitoring, trend analysis, or competitive intelligence.

3. Administrators:

- Personnel within organizations tasked with managing user access, setting configurations, and overseeing platform implementation to meet organizational objectives.

4. Developers and Integration Partners:

- Technical stakeholders who integrate the platform into existing systems or workflows, enabling seamless functionality within organizational processes.

5. Regulators and Auditors (indirect users):

- Entities conducting reviews to ensure the platform's compliance with global regulations and ethical standards.

Responsibilities of Users:

- Users are required to adhere to the terms of this Policy, including the ethical use of AI-generated outputs.
- Users must ensure that any data submitted to the Platform complies with applicable privacy and intellectual property laws.

Ownership of the AI Platform

The Platform, including all proprietary AI technologies, models, algorithms, and associated intellectual property (IP), is the exclusive property of InfoVision. This encompasses the entire ecosystem of AI-driven tools, methodologies, software infrastructure, and innovations developed by InfoVision to provide the services on the Platform.

Intellectual Property Rights:

- All patents, copyrights, trade secrets, and other IP rights associated with the Platform, including its AI capabilities and underlying code, are retained by InfoVision. These rights cannot be transferred or shared with users, unless explicitly stated in separate licensing agreements.
- Users are granted a non-exclusive, non-transferable license to use the Platform in accordance with the terms of this Policy, but this does not constitute any transfer of ownership rights over the AI or other Platform components.

Prohibited Activities:

- Any actions that involve reverse engineering, decompiling, modifying, or otherwise attempting to extract the source code or underlying logic of the AI models or Platform infrastructure are strictly prohibited.
- Unauthorized use, redistribution, or commercialization of the Platform's components is also forbidden. This includes the sharing of AI-generated outputs or derived technologies outside the scope of permitted usage.

Rights Reserved by InfoVision:

- InfoVision reserves the right to update, modify, or discontinue any component of the Platform at its discretion, ensuring that Users continue to benefit from the latest advancements in AI technology and services.
- In cases of violation of this Policy, InfoVision retains the right to suspend or terminate User access to the Platform and pursue legal actions if necessary.

Platform Access and Control:

- While Users retain ownership of the data they upload within the platform, they do not acquire ownership over the AI technologies, models, or algorithms that process, analyze, or generate insights from their data.
- The Platform is hosted and operated by InfoVision, who maintains control over all aspects of its operation, including the deployment of AI models, infrastructure, and data processing functions.

Scope of AI Use

The Platform integrates advanced AI and machine learning (ML) technologies to deliver actionable insights, streamline processes, and enhance user experience. The scope of AI use on the Platform is defined by its core functionalities, which are designed to serve a wide range of media intelligence needs while adhering to ethical standards and compliance requirements. The following outlines the primary areas of AI utilization:

1. **Data Processing and Analysis**

    - The Platform processes large volumes of structured and unstructured data from multiple sources, including social media, traditional news outlets, and industry reports. AI algorithms summarize this data to provide concise insights, highlight key trends, and facilitate informed decision-making.
    - AI models assess the credibility of data sources and identify false or misleading information to ensure users receive accurate and reliable insights.
    - Predictive analytics algorithms analyze historical data and current patterns to forecast emerging trends, enabling users to stay ahead in their respective industries.

2. **Text and Sentiment Analysis**

- The Platform leverages natural language processing (NLP) to evaluate the tone, emotion, and sentiment expressed in social media posts, articles, and other textual data.
- AI-powered thematic categorization organizes data into relevant topics, industries, or themes, making it easier for users to locate and analyze specific insights.

3. **Customization and Personalization**

- Automated alerts and notifications can be tailored to user-defined parameters, ensuring relevant updates are delivered promptly.

4. **Ethical and Regulatory Compliance**

- AI technologies on the Platform are specifically designed to comply with ethical standards and global regulatory requirements. This ensures:

  - **No Use of Harmful Content:** AI is prohibited from being used for harmful or unethical purposes, such as disinformation or violating privacy rights.
  - **Alignment with Industry Standards:** AI applications comply with GDPR, CCPA, and other relevant frameworks to ensure lawful use and data protection.

5. **User-Driven Enhancements**

- AI systems are continuously improved based on user feedback, ensuring the Platform evolves to meet changing needs and expectations.
- For Enterprise Clients, the Platform can integrate and deploy custom AI models tailored to specific organizational requirements, subject to compliance with InfoVision's terms of service.

6. **Limitations on Scope**

- The Platform's AI technologies are designed for specific use cases within media intelligence. Any attempt to repurpose or modify these technologies outside the intended scope (e.g., using them for non-media-related purposes) is strictly prohibited.
- The Platform relies on user-provided or publicly available data. InfoVision does not guarantee the accuracy of insights derived from incomplete or inaccurate input data.

Prohibited Actions

To ensure the ethical and lawful use of the Platform, certain actions are strictly prohibited. Users are not allowed to use the Platform for any unlawful purposes or in violation of applicable laws and regulations, including but not limited to activities that promote harm, discrimination, or illegal conduct. Unauthorized attempts to bypass, disable, or undermine the platform's security features or infrastructure are strictly forbidden. Users must refrain from submitting data that infringes upon

third-party intellectual property rights, violates privacy laws, or contains malicious content such as malware or viruses. Reverse engineering, decompiling, modifying, or otherwise tampering with the Platform's AI models, algorithms, or underlying technology is prohibited, as is any attempt to redistribute, resell, or commercialize the Platform or its outputs without explicit authorization. Additionally, the use of AI-generated insights to mislead, harm, or manipulate others, or in ways that conflict with user agreements or InfoVision's ethical principles, is not permitted. Any violations of these terms may result in immediate suspension or termination of access to the Platform and could lead to legal action.

Data Privacy and Security

The Platform is committed to safeguarding User data by adhering to data privacy and security standards in compliance with global regulations, including GDPR, CCPA, and the UK Data Protection Act. The Platform employs a data minimization approach, processing only essential information and anonymizing personal or sensitive data wherever applicable. All data is encrypted both at rest and in transit to prevent unauthorized access or breaches. Users' personally identifiable information (PII) is processed only with explicit consent, ensuring transparency and control over data usage. For added security, the Platform operates in secure, on-premises environments, ensuring no user data is transmitted to third-party servers. Rigorous measures, including access controls, regular audits, and advanced threat detection systems, are implemented to protect data integrity and confidentiality. InfoVision prioritizes User trust by maintaining a secure infrastructure that upholds the highest standards of data privacy and security throughout the Platform's operations.

Transparency and Accountability

- Users are notified when AI is used to generate insights or recommendations via an "AI Powered" label.
- AI-generated insights are provided for informational purposes only and do not constitute guarantees, warranties, or professional advice. We disclaim any liability for decisions made based on such insights, and users assume full responsibility for their interpretation and use.
- Any third-party AI services integrated into the Platform are vetted for compliance with privacy and ethical standards.

Ethical AI Principles

The Platform is guided by a commitment to developing and deploying AI technologies responsibly, ensuring fairness, transparency, and inclusiveness. The Platform strives to mitigate biases in training data and algorithms to provide equitable and accurate outputs for all users. Transparency is a core principle, with clear communication about the capabilities, limitations, and intended purposes of AI-driven features. Reliability is prioritized through continuous monitoring, rigorous testing, and regular updates to improve the accuracy and relevance of AI models. Inclusiveness

ensures that the Platform serves users across diverse geographies, industries, and demographics, fostering accessibility and equal opportunity. By adhering to these ethical principles, InfoVision ensures that the AI on Platform operates in alignment with global ethical standards, benefiting users while minimizing risks and promoting trust in AI-powered solutions.

Limitations of AI Use

The Platform acknowledges the inherent limitations of AI technologies to manage User expectations and promote responsible usage. AI-generated outputs may not always be fully accurate or complete, as models can misinterpret nuanced language, cultural references, or complex data. While designed for specific media intelligence use cases, performance outside these domains may be unreliable. Efforts are made to mitigate biases, but AI outputs may still reflect biases in training data, and insights depend on the accuracy and relevance of input data.

AI lacks human-level understanding of complex contexts, making independent verification of critical insights essential. InfoVision disclaims liability for decisions made solely on AI outputs, as the Platform is intended to assist rather than replace human expertise. Additionally, regulatory constraints, evolving technologies, resource dependencies, and potential service disruptions may impact functionality. Users are encouraged to interpret AI-generated insights carefully and apply their judgment to avoid unintended consequences.

Quality Assurance

The Platform maintains high standards of reliability, accuracy, and performance through a robust quality assurance framework. AI models are regularly tested, validated, and monitored in real-time to address inaccuracies, biases, or anomalies. Continuous updates and user feedback help improve model performance, while strict data validation ensures that only high-quality inputs are processed, supporting the platform’s.

Approval and Acknowledgements

All Users and stakeholders of the Platform must acknowledge and agree to the terms of this Policy before using the Platform. By accessing or using the Platform, Users consent to the processing of data, the use of AI-generated insights, and adherence to the Policy’s guidelines, including respecting intellectual property rights and compliance with data privacy standards.

Any significant changes to this Policy will prompt a re-acknowledgment from Users. Those who do not agree with the updated Policy may choose to discontinue use of the Platform.

Platform is committed to ensuring transparency, compliance, and ethical usage of AI technologies.

Updates to This Policy

The Platform is committed to keeping its Policy up to date to reflect evolving technologies, regulatory requirements, and best practices. As AI and related technologies advance, and as laws and regulations governing data privacy, security, and ethical AI usage evolve, this Policy may be revised to ensure continued compliance and alignment with industry standards.

Whenever there is a significant update or change to this Policy, Users will be notified through appropriate channels, such as email or Platform notifications or any other channel which may deem fit. These updates may include, but are not limited to, changes in the scope of AI usage, new data protection practices, enhancements to Platform features, or modifications in compliance with local or international regulations.

Users are encouraged to regularly review the Policy to stay informed about any modifications that may affect their use of the Platform. By continuing to use the Platform after updates are made, users agree to the revised policy. If any User does not agree with the updated Policy, they may choose to discontinue their use of the Platform.

The Platform strives to ensure that all updates are communicated transparently and implemented smoothly to maintain a secure, compliant, and User-friendly experience for all stakeholders.

Contact Information

For questions or concerns about this Policy, please contact:

Infovision, Inc.

Attn: AlphaMetricx Team

Email: contact@alphametricx.com

Phone: 469-619-3080

Website: https://alphametricx.com