MAIN SERVICE AGREEMENT
PUBLIC HEALTH 360

THIS MAIN SERVICES AGREEMENT GOVERNS THE CUSTOMER'S ACQUISITION AND USE OF PUBLIC HEALTH 360 ("PH360") SERVICES (THE "SERVICES") PROVIDED BY FLOURISH AND THRIVE LABS, LLC, AN ILLINOIS-BASED LIMITED LIABILITY COMPANY WITH AN OFFICE LOCATED AT 100 N ATKINSON ROAD #106-F, GRAYSLAKE, IL 60030 (THE "PROVIDER"). BY EXECUTING AN ORDER FORM THAT REFERENCES THIS AGREEMENT, THE CUSTOMER ACCEPTS THIS AGREEMENT IN ITS ENTIRETY. THE INDIVIDUAL ACCEPTING THIS AGREEMENT DOES SO ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, REPRESENTING THAT THEY HAVE THE AUTHORITY TO BIND SUCH AN ENTITY AND ITS AFFILIATES TO THESE TERMS AND CONDITIONS. THE TERM "CUSTOMER" REFERS TO SUCH AN ENTITY AND ITS AFFILIATES.

THE SERVICES MAY NOT BE ACCESSED FOR MONITORING THEIR AVAILABILITY, PERFORMANCE, FUNCTIONALITY, BENCHMARKING, OR OTHER COMPETITIVE PURPOSES. DIRECT COMPETITORS OF PH360 ARE PROHIBITED FROM ACCESSING THE SERVICES, EXCEPT WITH THE PROVIDER'S PRIOR WRITTEN CONSENT.

This agreement was last updated on October 1, 2025. It is effective between the Customer and the Provider as of the date of the Customer's accepting this agreement (the "Effective Date")

ARTICLE 1. DEFINITIONS

1.1. Definitions. As used in this Agreement, the following terms have the meanings set forth below:

1.1.1. **"Administrative Users"** means Customer's authorized personnel with administrative privileges to configure and manage the Services.

1.1.2. **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with a party, where "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity.

1.1.3. **"Agreement"** means this Main Service Agreement, together with all Order Forms, exhibits, schedules, and documents expressly incorporated by reference, all as may be amended from time to time.

1.1.4. **"AI System"** means the artificial intelligence technologies, including but not limited to machine learning models, natural language processing capabilities, and generative AI features, integrated into the Services.

1.1.5. **"Authorized Users"** means Customer's employees, contractors, and agents who are authorized by Customer to access and use the Services under Customer's subscription.

1.1.6. **"Business Associate Agreement" or "BAA"** means the separate agreement governing HIPAA-related obligations between the parties, if applicable.

1.1.7. **"Business Day"** means Monday – Friday.

1.1.8. **"Confidential Information"** means all non-public information disclosed by one party to the other party, whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure.

1.1.9. **"Customer Data"** means all electronic data, information, and materials provided, uploaded, or transmitted by or on behalf of Customer or Authorized Users to the Services, including Protected Health Information.

1.1.10. **"Data Processing Agreement" or "DPA"** means the separate agreement governing data protection obligations between the parties.

1.1.11. **"Documentation"** means Provider's standard user guides, technical documentation, and online help materials for the Services, as updated by Provider from time to time.

1.1.12. **"Emergency Maintenance"** means unscheduled maintenance required to address critical security vulnerabilities, significant performance degradation, or other urgent issues that may compromise the Services' security, stability, or availability.

1.1.13. **"Fees"** means the amounts payable by Customer to Provider for the Services as set forth in the applicable Order Form.

1.1.14. **"HIPAA"** means the Health Insurance Portability and Accountability Act of 1996, as amended, including the Health Information Technology for Economic and Clinical Health Act (HITECH Act), and their implementing regulations.

1.1.15. **"Incident"** means (i) any unauthorized access to, or acquisition, use, disclosure, or loss of Customer Data; (ii) any AI System malfunction that produces discriminatory, biased, or materially inaccurate outputs; or (iii) any other security breach affecting the Services.

1.1.16. **"Malicious Code"** means viruses, worms, time bombs, Trojan horses, and other harmful or malicious code, files, scripts, agents, or programs.

1.1.17. **"Module"** means a distinct functional component of PH360, including: (i) Maple (chat interface) - required for all subscriptions; (ii) Oak (chatbot builder); (iii) Ginkgo (knowledge base builder); and (iv) Cypress (Environmental Health Application, Permit, and Inspection).

1.1.18. **"NIST AI RMF"** means the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework (NIST AI 100-1 and subsequent versions), including all associated playbooks, profiles, and guidance documents.

1.1.19. **"Order Form"** means the ordering document executed by both parties that specifies the Services subscribed to, applicable Fees, term, and other subscription-specific details.

1.1.20. **"Production Environment"** means the Customer's live, operational instance of the Services used for actual operations, as distinguished from any testing or development environments.

1.1.21. **"Protected Health Information" or "PHI"** has the meaning set forth in HIPAA.

1.1.22. **"Scheduled Maintenance"** means planned maintenance activities for which Provider provides advance notice in accordance with Section 5.3.

1.1.23. **"Services"** means the PH360 cloud-based software applications and services provided by Provider to Customer pursuant to this Agreement, including the subscribed Modules, Documentation, and Support Services.

1.1.24. **"Service Commitment"** means Provider's commitment to maintain ninety-nine percent (99%) Monthly Uptime for the Services.

1.1.25. **"Support Services"** means the technical support services provided by Provider as described in the Support Plan Terms.

1.1.26. **"Terms of Service"** means the module-specific terms and conditions applicable to each subscribed Module.

1.1.27. **"Third-Party Services"** means any third-party products, services, or components integrated with or used in connection with the Services.

1.1.28. **"Unavailability"** means the inability of Authorized Users to access and use the Production Environment of the Services due to a failure of Provider's systems, excluding Excluded Downtime as defined in Article 5.

1.1.29. **"User"** means each individual Authorized User account established for access to the Services.

ARTICLE 2. SERVICES AND GRANT OF RIGHTS

2.1. **Provision of Services.** Subject to the terms and conditions of this Agreement, Provider shall make the Services available to Customer in accordance with the applicable Order Form(s). Provider shall provide the Services in a professional and workmanlike manner consistent with industry standards.

2.2. **License Grant.** Provider hereby grants to Customer, during the Term, a non-exclusive, non-transferable (except as expressly permitted herein), non-sublicensable (except to Affiliates and contractors solely for Customer's benefit) right to access and use the Services and Documentation solely for Customer's internal operations and in accordance with this Agreement and applicable Order Forms.

2.3. **Module Requirements.** Customer's subscription must include the Maple Module (chat interface), which is required for all PH360 implementations. Customer may additionally subscribe to one or more of the following optional Modules: Oak (chatbot builder), Ginkgo (knowledge base builder), and/or Cypress (Environmental Health Application, Permit, and Inspection). Each Module is subject to its respective Terms of Service.

2.4. **AI System Characteristics.** Customer acknowledges and agrees that:

- **2.4.1.** PH360 is an AI-first platform that utilizes artificial intelligence technologies throughout its functionality;
- **2.4.2.** AI Systems may produce outputs that vary based on inputs, context, and model behavior, and are not guaranteed to be error-free;
- **2.4.3.** AI System outputs should be subject to appropriate human review and oversight as required by Customer's policies and applicable law;
- **2.4.4.** Provider maintains AI governance practices aligned with the NIST AI RMF as described in Article 14.

2.5. **Service Limitations.** Provider reserves the right to:

- **2.5.1.** Modify the Services to comply with applicable law or improve functionality, provided that such modifications do not materially reduce the functionality described in the applicable Order Form;

2.5.2. Suspend access to the Services in accordance with Section 9.5 (Suspension Rights);

2.5.3. Impose reasonable usage limits or rate limits to ensure fair use and optimal performance for all customers.

2.6. Third-Party Services. The Services may integrate with or rely upon Third-Party Services. Provider makes no representations or warranties regarding Third-Party Services. Customer's use of Third-Party Services is subject to separate terms between Customer and the relevant third-party providers. Provider is not responsible for any unavailability, errors, or issues arising from Third-Party Services.

2.7. Subcontractors. Provider may use subcontractors to perform its obligations under this Agreement, provided that Provider remains responsible for the performance of such subcontractors and their compliance with the terms of this Agreement.

ARTICLE 3. CUSTOMER RESPONSIBILITIES AND USE RESTRICTIONS

3.1. Customer Responsibilities. Customer shall:

3.1.1. Provide accurate and complete information required for Service provisioning and account setup;

3.1.2. Maintain the security and confidentiality of all User credentials and access controls;

3.1.3. Promptly notify Provider of any unauthorized access to or use of the Services;

3.1.4. Ensure that Authorized Users comply with this Agreement and applicable law;

3.1.5. Maintain adequate internet connectivity, compatible devices, and other infrastructure necessary to access and use the Services;

3.1.6. Implement appropriate human oversight and review processes for AI System outputs, particularly for high-stakes decisions affecting public health, public policy, or criminal justice matters;

3.1.7. Comply with all applicable laws, regulations, and professional standards in its use of the Services, including but not limited to public health laws, data protection laws, and AI-related regulations;

3.2. Use Restrictions. Customer shall not, and shall ensure that Authorized Users do not:

3.2.1. Use the Services in any manner that violates applicable law or regulation;

3.2.2. Use the Services to transmit, store, or process Malicious Code;

3.2.3. Attempt to gain unauthorized access to the Services or related systems or networks;

3.2.4. Reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code or underlying algorithms of the Services (except to the extent such restriction is prohibited by applicable law);

3.2.5. Remove, alter, or obscure any proprietary notices on the Services or Documentation;

3.2.6. Use the Services to develop, train, or improve any competing product or service;

3.2.7. Share, resell, sublicense, or make the Services available to any third party (except as expressly permitted for Affiliates under Section 2.2);

3.2.8. Use automated means to access the Services except through documented APIs;

3.2.9. Interfere with or disrupt the integrity or performance of the Services;

3.2.10. Attempt to bypass or circumvent any security measures or usage limits;

3.2.11. Use the Services to process, store, or transmit content that is illegal, harmful, threatening, abusive, harassing, defamatory, or otherwise objectionable;

3.2.12. Use Customer Data or AI System outputs to intentionally train, fine-tune, or improve Provider's AI Systems without a separate written agreement;

3.2.13. Deliberately attempt to generate discriminatory, biased, or harmful outputs from the AI Systems;

3.2.14. Use the Services in a manner that violates the civil rights or privacy rights of individuals.

3.3. Authorized Users. Customer is responsible for all activities conducted under its account and by its Authorized Users. Customer shall ensure that Authorized Users are properly trained in the use of the Services and AI System outputs. Customer shall promptly notify Provider if Customer becomes aware of any violation of this Agreement by an Authorized User.

3.4. Data Accuracy and Quality. Customer is responsible for the accuracy, quality, and legality of Customer Data and the means by which Customer acquired such data. Customer represents and warrants that it has all necessary rights, consents, and authorizations to provide Customer Data to Provider and to permit Provider to process Customer Data as contemplated by this Agreement.

3.5. 3.5 Compliance with Government Procurement Laws. To the extent Customer is a governmental entity subject to procurement laws and regulations, Customer represents that it has complied with all applicable procurement requirements in entering into this Agreement.

ARTICLE 4. FEES AND PAYMENT

4.1. **Fees.** Customer shall pay Provider the Fees set forth in the applicable Order Form(s). Unless otherwise specified in an Order Form, all Fees are stated in United States Dollars and are non-refundable except as expressly provided in this Agreement.

4.2. **Payment Terms.** Unless otherwise specified in an Order Form:

- **4.2.1.** Fees for the initial Subscription Term shall be invoiced upon execution of the Order Form;
- **4.2.2.** Fees for subsequent Renewal Terms shall be invoiced at least thirty (30) days prior to the commencement of the Renewal Term;
- **4.2.3.** Payment is due within thirty (30) days of the invoice date;
- **4.2.4.** Payment shall be made by wire transfer, ACH, or other method mutually agreed upon by the parties.

4.3. **Late Payment.** If Customer fails to make any payment when due, Provider may, without limiting its other rights and remedies:

- **4.3.1.** Charge interest on the overdue amount at the rate of one and one-half percent (1.5%) per month (or the maximum rate permitted by law, if less), calculated daily and compounded monthly;
- **4.3.2.** Suspend access to the Services in accordance with Section 9.5 upon thirty (30) days' prior written notice;
- **4.3.3.** Terminate this Agreement in accordance with Article 9.

4.4. **Taxes.** All Fees are exclusive of all federal, state, local, and foreign taxes, levies, duties, or similar governmental assessments, including value-added, sales, use, and withholding taxes (collectively, "Taxes"). Customer is responsible for paying all Taxes associated with its purchases hereunder, excluding taxes based on Provider's net income. If Provider is obligated to collect or pay Taxes, the Taxes will be invoiced to Customer and Customer will pay such Taxes unless Customer provides Provider with a valid tax exemption certificate.

4.5. **Fee Adjustments.** Provider may increase Fees for any Renewal Term up to five percent (5%) by providing Customer with at least ninety (90) days' prior written notice before the commencement of the Renewal Term. If Customer does not agree to the fee increase, Customer may terminate this Agreement by providing written notice to Provider at least thirty (30) days prior to the commencement of the Renewal Term.

4.6. **Governmental Appropriations.** If Customer is a governmental entity whose payment obligations are subject to annual appropriations:

- **4.6.1.** This Agreement is subject to the availability of appropriated funds, and no provision herein shall be interpreted to require obligation or payment of funds in violation of applicable law;
- **4.6.2.** If funds are not appropriated or otherwise made available to support continuation of performance in a subsequent fiscal year, Customer may terminate this Agreement at the end of the current fiscal year upon thirty (30) days' prior written notice to Provider;
- **4.6.3.** Customer shall use commercially reasonable efforts to secure continued appropriations and shall promptly notify Provider if appropriations are not secured.

ARTICLE 5. SERVICE LEVELS

5.1. **Service Commitment.** Provider commits to maintaining the Services with a Monthly Uptime Percentage of at least ninety-nine percent (99%) ("Service Commitment"). "Monthly Uptime Percentage" is calculated as: [(Total Minutes in Month - Minutes of Unavailability) / Total Minutes in Month] × 100.

5.2. **Service Credits.** If Provider fails to meet the Service Commitment in any calendar month, and provided Customer has met the requirements in Section 5.6, Customer will be eligible to receive Service Credits as follows:

Monthly Uptime Percentage	Service Credit (% of Monthly Fees)
98.0% to < 99.0%	5%
98.0% to < 99.0%	10%
97.0% to < 98.0%	15%
95.0% to < 97.0%	25%
< 95.0%	50%

Service Credits represent Customer's sole and exclusive remedy for Provider's failure to meet the Service Commitment, unless otherwise provided in an Addendum to this Agreement.

5.3. **Excluded Downtime.** The following shall not be considered Unavailability for purposes of calculating Monthly Uptime Percentage ("Excluded Downtime"):

5.3.1. **Scheduled Maintenance:** Planned maintenance performed during the Maintenance Windows described below, provided Provider gives at least two (2) business days advance notice;

5.3.2. **Emergency Maintenance:** Unscheduled maintenance necessary to address critical security vulnerabilities or significant performance issues, for which Provider shall use commercially reasonable efforts to provide advance notice;

5.3.3. **Customer-Caused Issues:** Unavailability caused by Customer's or its Authorized Users' actions, misconfigurations, or use of the Services in violation of this Agreement or the Documentation;

5.3.4. **Third-Party Services:** Unavailability caused by Third-Party Services or third-party network connectivity issues beyond Provider's reasonable control;

5.3.5. **Force Majeure:** Unavailability caused by Force Majeure events as defined in Section 12.11;

5.3.6. **Internet Connectivity:** Issues with Customer's internet service provider or general internet connectivity issues outside Provider's network;

5.3.7. **Customer Equipment:** Issues with Customer's hardware, software, or network infrastructure used to access the Services;

5.3.8. **Suspension:** Unavailability resulting from suspension of Services in accordance with Section 9.5.

5.4. **Maintenance Windows.** Provider's standard maintenance windows are:

5.4.1. **Scheduled Maintenance: Saturdays from 12:00 AM to 6:00 AM Central Time.** Provider will use commercially reasonable efforts to minimize disruption during these windows. Provider may schedule additional maintenance windows with at least two (2) business days advance notice

5.5. **Monitoring and Reporting.** Provider maintains monitoring systems to track Service availability. Customer may request uptime reports on a quarterly basis.

5.6. **Service Credit Requests.** To receive a Service Credit:

5.6.1. Customer must submit a written request to Provider within thirty (30) days following the end of the month in which Unavailability occurred;

5.6.2. The request must include: (i) the subject line "SLA Credit Request"; (ii) the dates and times of each Unavailability incident; (iii) logs, screenshots, or other evidence documenting the Unavailability; and (iv) the affected Users and locations;

5.6.3. Customer must have paid all undisputed Fees when due;

5.6.4. Provider will review the request in good faith and issue approved Service Credits within the next billing cycle;

5.6.5. Service Credits may only be applied toward future Fees for the Services or an extension of the current Services and cannot be redeemed for cash;

5.7. **Termination Right for Repeated Failures.** If Provider fails to meet the Service Commitment for three (3) or more months in any consecutive six (6) month period, and such failures are not substantially due to Excluded Downtime, Customer may terminate this Agreement upon thirty (30) days' written notice to Provider. Upon such termination, Provider shall refund to Customer a pro-rata portion of prepaid Fees for the terminated portion of the Subscription Term.

ARTICLE 6. DATA PROTECTION AND SECURITY

6.1. **Customer Data Ownership.** As between the parties, Customer retains all right, title, and interest in and to Customer Data. Customer hereby grants Provider a non-exclusive, worldwide, royalty-free license to host, copy, transmit, display, and process Customer Data solely to the extent necessary to provide the Services and perform Provider's obligations under this Agreement.

6.2. **Data Protection Obligations.** The parties shall comply with their respective obligations under the Data Processing Agreement (DPA) (or executed separately) regarding the processing of personal information, including Protected Health Information if applicable.

6.3. **HIPAA Compliance.** If Customer Data includes Protected Health Information, the parties shall execute and comply with the Business Associate Agreement (BAA) (executed separately).

6.4. **Security Measures.** Provider shall implement and maintain administrative, physical, and technical safeguards designed to:

6.4.1. Protect the security, confidentiality, and integrity of Customer Data;

6.4.2. Protect against anticipated threats or hazards to the security or integrity of Customer Data;

6.4.3. Protect against unauthorized access to or use of Customer Data;

6.4.4. Ensure the ongoing confidentiality, integrity, availability, and resilience of Provider's systems and services.

Provider's current security measures are described in Provider's Security Documentation, available upon request at https://trust.fandtlabs.com and subject to Provider's confidentiality requirements.

6.5. **Data Location.** Provider will store and process Customer Data within the United States unless otherwise specified in an Order Form. Provider will not transfer Customer Data outside the United States without Customer's prior written consent, except as required by law.

6.6. **Data Backup and Recovery.** Provider shall:

- **6.6.1.** Maintain regular backups of Customer Data in accordance with industry standards;
- **6.6.2.** Implement and maintain disaster recovery procedures designed to recover Customer Data in the event of a system failure;
- **6.6.3.** Provide Customer with reasonable assistance in recovering Customer Data in the event of data loss, subject to the limitations in Article 11.

6.7. **Incident Response.** Provider shall:

- **6.7.1.** Maintain an incident response plan and security incident management procedures;
- **6.7.2.** Promptly investigate any Incident and take appropriate measures to mitigate and remediate such Incident;
- **6.7.3.** Notify Customer without undue delay, and in any event within two (2) business days of becoming aware of any Incident that affects Customer Data or the Services, unless a shorter time period is required by applicable law;
- **6.7.4.** Provide Customer with sufficient information about the Incident to enable Customer to meet any notification obligations under applicable law;
- **6.7.5.** Cooperate with Customer's reasonable requests for information and assistance related to the Incident.

6.8. **Subprocessors.** Provider may engage subprocessors to process Customer Data, subject to the terms of the Data Processing Agreement. Provider maintains a current list of subprocessors, which is available to the Customer upon request at https://trust.fandtlabs.com.

6.9. **Security Audits and Certifications.**** Provider maintains compliance with industry-standard security frameworks and undergoes regular third-party security audits. Provider's current security certifications include SOC 2 Type II. Customer may request summary audit documentation upon request at https://trust.fandtlabs.com. Access to summary audit reports subject to Provider's confidentiality requirements.

6.10. **Customer Security Obligations.** Customer shall:

- **6.10.1.** Use commercially reasonable efforts to prevent unauthorized access to or use of the Services;
- **6.10.2.** Promptly notify Provider of any security breach or unauthorized access;
- **6.10.3.** Implement and maintain appropriate security measures for Customer's systems, networks, and devices used to access the Services;
- **6.10.4.** Ensure that Authorized Users maintain the confidentiality of their credentials.

ARTICLE 7. INTELLECTUAL PROPERTY RIGHTS

7.1. **Provider IP Rights.** As between the parties, Provider retains all right, title, and interest in and to:

- **7.1.1.** The Services, including all software, applications, AI Systems, algorithms, models, technologies, and Documentation;
- **7.1.2.** All modifications, improvements, and derivative works of the foregoing;
- **7.1.3.** All Provider Confidential Information;
- **7.1.4.** All intellectual property rights in the foregoing.

Nothing in this Agreement grants Customer any rights in Provider's intellectual property except the limited license granted in Section 2.2.

7.2. **Customer IP Rights.** As between the parties, Customer retains all right, title, and interest in and to Customer Data and Customer's Confidential Information.

7.3. **Feedback.** If Customer provides Provider with any suggestions, comments, feedback, or ideas regarding the Services ("Feedback"), Provider may use such Feedback without obligation or restriction. Customer hereby grants Provider a worldwide, perpetual, irrevocable, royalty-free license to use, reproduce, modify, create derivative works from, distribute, and otherwise exploit such Feedback for any purpose.

7.4. **Usage Data.** Provider may collect and analyze technical and operational data regarding Customer's use of the Services, including performance metrics, usage statistics, and error reports, in aggregated and de-identified form ("Usage Data"). Provider may use Usage Data to:

- **7.4.1.** Operate, maintain, and improve the Services;
- **7.4.2.** Develop new features and services;
- **7.4.3.** Generate industry benchmarks and statistical analyses;
- **7.4.4.** Comply with legal obligations.

Provider will not disclose Usage Data in a manner that identifies Customer without Customer's prior written consent, except as required by law.

7.5. **AI Model Training Restrictions.** Unless otherwise agreed in writing, Provider shall not use Customer Data to train, fine-tune, or otherwise improve Provider's AI Systems or develop new AI models, except to the extent necessary to provide the Services to Customer.

7.6. **Open Source Software.** The Services may incorporate or be distributed with open source software components. Such open source components are licensed under their respective open source licenses and not under the terms of this Agreement. Provider makes no warranties or representations regarding open source components.

ARTICLE 8. WARRANTIES AND DISCLAIMERS

8.1. **Mutual Warranties.** Each party represents and warrants that:

- **8.1.1.** It has the legal authority to enter into this Agreement;
- **8.1.2.** This Agreement constitutes a valid and binding obligation, enforceable in accordance with its terms;
- **8.1.3.** The execution and performance of this Agreement does not violate any agreement, law, or regulation to which it is subject;
- **8.1.4.** It will comply with all applicable laws and regulations in performing its obligations under this Agreement.

8.2. **Provider Warranties.** Provider represents and warrants that:

- **8.2.1.** **Performance Standard.** The Services will perform materially in accordance with the Documentation and this Agreement;
- **8.2.2.** **Professional Standards.** Provider will provide the Services in a professional and workmanlike manner consistent with industry standards;
- **8.2.3.** **Malicious Code.** Provider will use commercially reasonable efforts to ensure the Services do not contain Malicious Code. Provider will use industry-standard anti-virus and anti-malware software;
- **8.2.4.** **No Unauthorized Access.** Provider has not and will not knowingly enable any third party to access Customer Data except as required to provide the Services or as required by law;
- **8.2.5.** **Legal Compliance.** The Services comply in all material respects with applicable U.S. federal and state laws as of the Effective Date.

8.3. **Remedy for Breach of Provider Warranties.** For any breach of the warranties in Section 8.2, Customer's exclusive remedy shall be for Provider to:

- **8.3.1.** Re-perform the non-conforming Services; or
- **8.3.2.** If Provider cannot substantially correct the breach within thirty (30) days after receipt of written notice, Customer may terminate the affected Order Form and receive a pro-rata refund of prepaid Fees for the terminated portion of the Subscription Term.

8.4. **Customer Warranties.** Customer represents and warrants that:

- **8.4.1.** Customer has all necessary rights, consents, and authorizations to provide Customer Data to Provider and to permit Provider to use Customer Data as contemplated by this Agreement;
- **8.4.2.** Customer Data does not and will not violate any law or infringe any third-party rights;
- **8.4.3.** Customer will use the Services in compliance with all applicable laws, regulations, and professional standards;
- **8.4.4.** If Customer is a governmental entity, Customer has complied with all applicable procurement laws and regulations.

8.5. **DISCLAIMER OF WARRANTIES. EXCEPT AS EXPRESSLY PROVIDED IN THIS ARTICLE 8, PROVIDER MAKES NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, AND PROVIDER SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. WITHOUT LIMITING THE FOREGOING:**

- **8.5.1.** **PROVIDER DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR COMPLETELY SECURE, OR THAT ALL DEFECTS WILL BE CORRECTED;**
- **8.5.2.** **PROVIDER DOES NOT WARRANT THAT THE AI SYSTEMS WILL PRODUCE ACCURATE, COMPLETE, OR ERROR-FREE OUTPUTS IN ALL CASES. CUSTOMER ACKNOWLEDGES THAT AI SYSTEMS MAY PRODUCE INCORRECT, INCOMPLETE, BIASED, OR UNEXPECTED OUTPUTS AND THAT HUMAN OVERSIGHT AND REVIEW ARE ESSENTIAL;**
- **8.5.3.** **PROVIDER DOES NOT WARRANT THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION OR OUTPUT PROVIDED BY THE SERVICES, INCLUDING AI-GENERATED CONTENT;**
- **8.5.4.** **PROVIDER IS NOT RESPONSIBLE FOR ANY DELAYS, FAILURES, INTERRUPTIONS, OR ERRORS CAUSED BY THIRD-PARTY SERVICES, CUSTOMER'S INTERNET CONNECTION, OR OTHER FACTORS OUTSIDE PROVIDER'S REASONABLE CONTROL;**

8.5.5. THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE."

8.6. AI System Limitations Acknowledgment. Customer specifically acknowledges and agrees that:

8.6.1. AI Systems are based on statistical models and machine learning technologies that may produce variable outputs;

8.6.2. AI System outputs may reflect biases present in training data, despite Provider's efforts to mitigate such biases;

8.6.3. AI Systems should not be relied upon as the sole basis for high-stakes decisions affecting individuals' health, safety, legal status, or civil rights without appropriate human review and oversight;

8.6.4. Provider's AI governance practices are designed to align with the NIST AI RMF but do not guarantee error-free or bias-free outputs;

8.6.5. Customer is responsible for implementing appropriate validation, testing, and oversight procedures for its use of AI System outputs.

ARTICLE 9. TERM AND TERMINATION

9.1. Initial Term. This Agreement commences on the Effective Date and continues for an initial term of twelve (12) months (the "Initial Term") unless earlier terminated in accordance with this Article 9.

9.2. Renewal Terms. Following the Initial Term, this Agreement will automatically renew for successive twelve (12) month periods (each a "Renewal Term," and together with the Initial Term, the "Subscription Term") unless either party provides written notice of non-renewal at least sixty (60) days prior to the end of the then-current Subscription Term.

9.3. Termination for Cause. Either party may terminate this Agreement upon written notice if the other party:

9.3.1. Materially breaches this Agreement and fails to cure such breach within thirty (30) days after receiving written notice thereof (or ten (10) days for payment breaches); or

9.3.2. Becomes insolvent, makes an assignment for the benefit of creditors, or becomes subject to any proceedings under any bankruptcy or insolvency law.

9.4. Suspension Rights. Provider may suspend Customer's access to the Services immediately upon notice if:

9.4.1. Customer's account is more than thirty (30) days overdue;

9.4.2. Customer's use of the Services: (i) poses a security risk to the Services or any third party; (ii) may adversely impact the Services or Provider's systems or networks; (iii) may subject Provider to liability; or (iv) violates applicable law;

9.4.3. Customer is in material breach of Article 3 (Customer Responsibilities and Use Restrictions).

Provider will use commercially reasonable efforts to provide notice of suspension and an opportunity to remedy the issue before suspension, except in cases of emergency or security threats where immediate suspension is necessary.

9.5. Effect of Termination. Upon expiration or termination of this Agreement:

9.5.1. All rights granted to Customer under this Agreement will immediately cease;

9.5.2. Customer shall immediately discontinue all use of the Services;

9.5.3. Each party shall return or destroy all Confidential Information of the other party in its possession or control, except as required by law, Addenda to this agreement, or professional obligations;

9.5.4. Customer shall pay all outstanding Fees and charges accrued through the effective date of termination;

9.5.5. Provider shall cooperate with Customer's reasonable requests for data retrieval during the Data Retention Period described in Section 9.7.

9.6. Data Retrieval and Deletion.

9.6.1. Data Retention Period: Following termination or expiration, Provider will make Customer Data available for retrieval for a period of sixty (60) days (the "Data Retention Period"). Customer may request export of Customer Data during this period by contacting Provider's support team.

9.6.2. Data Export Format: Provider will provide Customer Data in a commonly used electronic format (e.g., JSON, CSV, or XML as appropriate for the data type). Provider may charge reasonable fees for complex or extensive data export requests.

9.6.3. Data Deletion: Following the Data Retention Period, or upon Customer's earlier written request, Provider will delete or destroy all Customer Data in its possession or control, except as required by law, regulation, Addenda to this agreement, or professional obligations. Provider will provide written certification of deletion upon Customer's request.

9.6.4. Backup Deletion: Customer Data stored in Provider's backups will be deleted in accordance with Provider's standard backup retention and deletion procedures, which may result in retention beyond the Data Retention Period. Provider will not restore Customer Data from backups after the Data Retention Period except as required by law.

9.7. **Survival.** The following provisions shall survive expiration or termination of this Agreement: Articles 1 (Definitions), 4.1 and 4.3 (payment obligations accrued prior to termination), 6.1 (Customer Data Ownership), 6.9 (Data Deletion obligations), 7 (Intellectual Property Rights), 8.5 (Disclaimer), 9.6-9.7 (Effect of Termination provisions), 10 (Confidentiality), 11 (Limitation of Liability), 12.1 (Indemnification - to the extent related to pre-termination activities), and 12 (General Provisions).

ARTICLE 10. CONFIDENTIALITY

10.1. **Confidential Information.** Each party (the "Receiving Party") agrees to hold in confidence and not disclose to any third party any Confidential Information of the other party (the "Disclosing Party"), except as expressly permitted in this Agreement. The Receiving Party shall:

10.1.1. Use the same degree of care to protect the Disclosing Party's Confidential Information as it uses to protect its own confidential information of similar nature, but in no event less than reasonable care;

10.1.2. Use the Disclosing Party's Confidential Information solely for the purposes of performing its obligations or exercising its rights under this Agreement;

10.1.3. Limit disclosure of the Disclosing Party's Confidential Information to its employees, contractors, and advisors who have a legitimate need to know and who are bound by confidentiality obligations at least as protective as those in this Agreement.

10.2. **Exceptions.** Confidential Information does not include information that:

10.2.1. Is or becomes publicly available through no breach of this Agreement by the Receiving Party;

10.2.2. Was rightfully known to the Receiving Party without obligation of confidentiality prior to disclosure by the Disclosing Party;

10.2.3. Is rightfully received by the Receiving Party from a third party without breach of any confidentiality obligation;

10.2.4. Is independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information.

10.3. **Compelled Disclosure.** If the Receiving Party is compelled by law, regulation, court order, or governmental authority to disclose the Disclosing Party's Confidential Information, the Receiving Party shall:

10.3.1. Promptly notify the Disclosing Party of such requirement (unless prohibited by law);

10.3.2. Cooperate with the Disclosing Party's reasonable efforts to seek a protective order or other appropriate remedy;

10.3.3. Disclose only that portion of the Confidential Information that is legally required to be disclosed;

10.3.4. Use commercially reasonable efforts to obtain confidential treatment for any Confidential Information that is disclosed.

10.4. **Public Records.** If Customer is a governmental entity subject to public records laws, Customer acknowledges that this Agreement and certain related records may be subject to public disclosure. To the extent permitted by law:

10.4.1. Provider may designate certain information as confidential and proprietary in accordance with applicable public records laws;

10.4.2. Customer shall promptly notify Provider upon receipt of any public records request that seeks disclosure of Provider's Confidential Information;

10.4.3. Customer shall cooperate with Provider's reasonable efforts to protect such information from disclosure, including asserting applicable exemptions;

10.4.4. If disclosure is required, Customer shall provide Provider with reasonable advance notice and disclose only that portion of Provider's Confidential Information that is legally required.

10.5. **Term of Confidentiality Obligations.** The confidentiality obligations in this Article 10 shall continue for a period of five (5) years from the date of disclosure of the relevant Confidential Information, except that confidentiality obligations with respect to trade secrets shall continue for so long as such information remains a trade secret under applicable law.

ARTICLE 11. LIMITATION OF LIABILITY

11.1. **LIMITATION OF CONSEQUENTIAL DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES, INCLUDING DAMAGES FOR LOSS OF PROFITS, REVENUE, BUSINESS OPPORTUNITIES, GOODWILL, USE, OR DATA, ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE SERVICES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF THE LEGAL THEORY UNDER WHICH LIABILITY IS ASSERTED (WHETHER CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY, OR OTHERWISE).**

11.2. CAP ON LIABILITY. EXCEPT AS PROVIDED IN SECTION 11.3, EACH PARTY'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY, OR OTHERWISE, SHALL NOT EXCEED THE TOTAL FEES PAID OR PAYABLE BY CUSTOMER TO PROVIDER UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO LIABILITY.

11.3. Exceptions to Liability Limitations. The limitations of liability in Sections 11.1 and 11.2 shall not apply to:

- **11.3.1.** Either party's indemnification obligations under Article 12;
- **11.3.2.** Either party's gross negligence, willful misconduct, or fraud;
- **11.3.3.** Either party's breach of Article 10 (Confidentiality);
- **11.3.4.** Customer's payment obligations;
- **11.3.5.** Violations of the other party's intellectual property rights;
- **11.3.6.** Liabilities that cannot be limited under applicable law.

11.4. Government Entity Considerations. If Customer is a governmental entity:

- **11.4.1.** Nothing in this Agreement shall be interpreted as requiring Customer to indemnify or hold harmless Provider to the extent prohibited by law;
- **11.4.2.** To the extent permitted by applicable law, the liability limitations in this Article 11 apply to Customer's obligations, except where such limitations are prohibited by law;
- **11.4.3.** Customer's liability is subject to the limitations and requirements of applicable law, including sovereign immunity and statutory limits on governmental liability, where applicable.

11.5. Basis of the Bargain. The parties acknowledge and agree that the limitations of liability set forth in this Article 11 are fundamental elements of the basis of the bargain between the parties, and that the Fees reflect the allocation of risk set forth in this Agreement. The limitations of liability in this Article 11 shall apply even if any limited remedy provided herein fails of its essential purpose.

ARTICLE 12. INDEMNIFICATION

12.1. Provider Indemnification. Provider shall defend Customer against any third-party claim that the Services, when used in accordance with this Agreement, infringe or misappropriate a U.S. patent, copyright, trademark, or trade secret, and shall indemnify and hold harmless Customer from and against any damages, costs, and attorneys' fees finally awarded against Customer or agreed to in settlement by Provider with respect to such claim, provided that Customer:

- **12.1.1.** Promptly notifies Provider in writing of the claim;
- **12.1.2.** Grants Provider sole control of the defense and settlement of the claim;
- **12.1.3.** Provides Provider with reasonable cooperation and assistance in the defense of the claim.

12.2. Provider Indemnification Exclusions. Provider's indemnification obligation under Section 12.1 shall not apply to claims arising from:

- **12.2.1.** Modifications to the Services not made or authorized by Provider;
- **12.2.2.** Use of the Services in combination with products, services, data, or materials not provided by Provider, if the infringement would not have occurred but for such combination;
- **12.2.3.** Use of the Services in a manner not authorized by this Agreement or the Documentation;
- **12.2.4.** Customer Data or any content provided by Customer;
- **12.2.5.** Third-Party Services;
- **12.2.6.** Failure to implement updates or patches provided by Provider, if such updates or patches would have avoided the infringement.

12.3. Provider Remedies for Infringement Claims. If the Services are, or in Provider's opinion are likely to be, subject to a claim of infringement, Provider may, at its option and expense:

- **12.3.1.** Procure for Customer the right to continue using the Services;
- **12.3.2.** Replace or modify the Services to make them non-infringing while providing materially equivalent functionality; or
- **12.3.3.** If neither 12.3.1 nor 12.3.2 is commercially reasonable, terminate the affected Order Form and refund to Customer a pro-rata portion of prepaid Fees for the terminated portion of the Subscription Term.

12.4. Customer Indemnification. Customer shall defend Provider against any third-party claim arising from or related to:

- **12.4.1.** Customer Data, including claims that Customer Data infringes or misappropriates any third-party intellectual property rights or violates applicable law;
- **12.4.2.** Customer's use of the Services in violation of this Agreement or applicable law;
- **12.4.3.** Customer's combination of the Services with other products, services, or content not provided by Provider, if the claim would not have arisen but for such combination;

and shall indemnify and hold harmless Provider from and against any damages, costs, and attorneys' fees finally awarded against Provider or agreed to in settlement by Customer with respect to such claim, provided that Provider:

12.4.4. Promptly notifies Customer in writing of the claim;

12.4.5. Grants Customer sole control of the defense and settlement of the claim (provided that Customer may not settle any claim in a manner that admits fault on behalf of Provider or imposes obligations on Provider without Provider's prior written consent);

12.4.6. Provides Customer with reasonable cooperation and assistance in the defense of the claim.

12.5. **Government Entity Indemnification Limitations.** Notwithstanding anything to the contrary in this Article 12, if Customer is a governmental entity:

12.5.1. Customer's indemnification obligations in Section 12.4 shall apply only to the extent permitted by applicable law;

12.5.2. Customer shall not be required to indemnify Provider for claims arising from Provider's negligence or willful misconduct;

12.5.3. Customer's indemnification obligations are subject to the limitations of sovereign immunity, statutory immunity, and other limitations on governmental liability under applicable law;

12.5.4. Nothing in this Agreement shall be construed as a waiver of sovereign immunity or other immunities available to Customer under applicable law.

12.6. **Sole Remedy.** THIS ARTICLE 12 STATES EACH PARTY'S SOLE AND EXCLUSIVE REMEDY AND THE OTHER PARTY'S ENTIRE LIABILITY FOR ANY INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS.

ARTICLE 13. GENERAL PROVISIONS

13.1. **Entire Agreement.** This Agreement, including all Order Forms, exhibits, and documents incorporated by reference, constitutes the entire agreement between the parties regarding the subject matter hereof and supersedes all prior and contemporaneous agreements, proposals, or representations, written or oral, concerning such subject matter. In the event of any conflict between the terms of this Agreement and any Order Form, the Order Form shall control solely with respect to the specific Services described in such Order Form.

13.2. **Amendment.** Provider may update or modify the terms of this Agreement, the Documentation, or Provider's policies from time to time. Provider will provide notice of material changes by:

13.2.1. Posting the updated terms on Provider's website; and

13.2.2. Sending notice to Customer's designated contact email address.

Material changes will become effective thirty (30) days after notice is provided. Customer's continued use of the Services after the effective date of changes constitutes acceptance of the modified terms. If Customer does not agree to the modified terms, Customer may terminate this Agreement in accordance with Section 9.3.

13.3. **Waiver.** No waiver of any provision of this Agreement shall be effective unless in writing and signed by the party against whom such waiver is sought to be enforced. No failure or delay by either party in exercising any right or remedy under this Agreement shall operate as a waiver thereof, nor shall any single or partial exercise of any right or remedy preclude any other or further exercise thereof.

13.4. **Severability.** If any provision of this Agreement is held by a court of competent jurisdiction to be invalid, illegal, or unenforceable, the remaining provisions shall continue in full force and effect, and such provision shall be modified to the minimum extent necessary to make it valid and enforceable while preserving the parties' original intent.

13.5. **Assignment.**

13.5.1. Neither party may assign this Agreement or any of its rights or obligations hereunder without the prior written consent of the other party, except that either party may assign this Agreement:

13.5.1.1. To an Affiliate, provided the assigning party provides written notice to the other party and the Affiliate agrees in writing to be bound by the terms of this Agreement; or

13.5.1.2. In connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets, provided the assignee agrees in writing to be bound by the terms of this Agreement.

13.5.2. Any attempted assignment in violation of this Section 13.5 shall be void.

13.5.3. This Agreement shall be binding upon and inure to the benefit of the parties and their respective permitted successors and assigns.

13.6. **Notices.**

13.6.1. All notices required or permitted under this Agreement shall be in writing and shall be deemed given:

13.6.1.1. When delivered personally;

13.6.1.2. Three (3) business days after being sent by certified or registered mail, return receipt requested, postage prepaid;

13.6.1.3. One (1) business day after being sent by a nationally recognized overnight courier service; or

13.6.1.4. When sent by email with confirmation of receipt, provided that notices of termination or breach must also be sent by certified mail or overnight courier.

13.6.2. Notices to Provider shall be sent to:

Flourish and Thrive Labs, LLC

100 N Atkinson Road #106-F

Grayslake, IL 60030

Email: juliana@fandtlabs.com

Attention: Legal Department

13.6.3. Notices to Customer shall be sent to the address and email provided in the applicable Order Form or as otherwise updated by Customer in writing.

13.7. Independent Contractors. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the parties. Neither party has the authority to bind the other or to incur obligations on behalf of the other without the other party's prior written consent.

13.8. Governing Law and Jurisdiction.

13.8.1. Governing Law: This Agreement shall be governed by and construed in accordance with the laws of the State of Illinois and the laws of the United States of America, without regard to conflicts of law principles that would require the application of the laws of another jurisdiction.

13.8.2. Jurisdiction and Venue: Any legal action or proceeding arising under or relating to this Agreement shall be brought exclusively in the federal or state courts located in Lake County, Illinois, and each party irrevocably submits to the exclusive jurisdiction of such courts in any such action or proceeding. Notwithstanding the foregoing, either party may seek injunctive or other equitable relief in any court of competent jurisdiction.

13.8.3. Government Entity Exception: If Customer is a governmental entity whose laws require that disputes be resolved in a specific forum, then such requirements shall govern, and this Section 13.8 shall be modified to the minimum extent necessary to comply with such requirements.

13.9. Compliance with Laws. Each party shall comply with all applicable federal, state, and local laws, regulations, and ordinances in connection with its performance under this Agreement, including export control laws, anti-corruption laws, and privacy laws.

13.10. Export Compliance. Customer acknowledges that the Services and related technical data may be subject to U.S. export control laws and regulations. Customer shall not, directly or indirectly, export, re-export, or transfer the Services or technical data to any prohibited country, entity, or person, or for any prohibited end use, without obtaining all required government authorizations.

13.11. Force Majeure. Neither party shall be liable for any failure or delay in performance under this Agreement (except for payment obligations) to the extent such failure or delay is caused by circumstances beyond the reasonable control of such party, including acts of God, natural disasters, war, terrorism, riots, embargoes, acts of civil or military authorities, fire, floods, accidents, pandemics, strikes, alien invasions, zombie apocalypses, rapture, or shortages of transportation facilities, fuel, energy, labor, or materials ("Force Majeure Event"). The affected party shall:

13.11.1. Promptly notify the other party of the Force Majeure Event;

13.11.2. Use commercially reasonable efforts to mitigate the effects of the Force Majeure Event;

13.11.3. Resume performance as soon as reasonably practicable after the Force Majeure Event ceases.

If a Force Majeure Event continues for more than sixty (60) days, either party may terminate this Agreement upon written notice to the other party.

13.12. Counterparts. This Agreement, Order Forms, Addendums, or other documents may be executed in counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same instrument. Electronic signatures shall have the same legal effect as original signatures.

13.13. Third-Party Beneficiaries. This Agreement is intended solely for the benefit of the parties hereto and their permitted successors and assigns, and nothing in this Agreement shall confer upon any other person or entity any right, benefit, or remedy of any nature whatsoever.

13.14. Order of Precedence. In the event of any conflict or inconsistency between the documents comprising this Agreement, the following order of precedence shall apply (from highest to lowest):

13.14.1. Order Forms (for the specific Services described therein);

13.14.2. Business Associate Agreement (if applicable);

13.14.3. Data Processing Agreement;

13.14.4. This Main Service Agreement;

13.14.5. Module-specific Terms of Service;

13.14.6. Support Plan Terms;

13.14.7. Documentation.

13.15. Publicity. Neither party shall use the other party's name, logo, or trademarks in any publicity, advertising, or promotional materials without the prior written consent of the other party, except that Provider may identify Customer as a customer of Provider in Provider's marketing materials and on Provider's website unless Customer notifies Provider in writing that it objects to such use.

13.16. Government Contract Requirements. If Customer is a governmental entity and this Agreement is subject to specific government contract requirements, regulatory provisions, or statutory requirements, the parties agree to work cooperatively to incorporate such requirements through an addendum to this Agreement or Order Form, provided such requirements do not materially alter the fundamental terms of this Agreement.

13.17. Audit Rights. Upon reasonable advance written notice (at least fifteen (15) business days), Customer may, at its own expense and no more than once per calendar year, audit Provider's compliance with this Agreement, including security and data protection obligations. Such audits shall:

13.17.1. Be conducted during normal business hours and in a manner that does not unreasonably interfere with Provider's business operations;

13.17.2. Be subject to Provider's security and confidentiality requirements;

13.17.3. Be limited in scope to matters directly related to Provider's obligations under this Agreement;

13.17.4. Be conducted by an independent third-party auditor reasonably acceptable to Provider if the audit involves access to Provider's systems, facilities, or confidential information.

Provider may satisfy audit requirements by providing Customer with current security audit reports (e.g., SOC 2 Type II reports) or certifications prepared by independent third-party auditors.

ARTICLE 14. AI-SPECIFIC PROVISIONS

14.1. NIST AI RMF Alignment.

14.1.1. Governance Commitment. Provider maintains AI governance practices designed to align with the NIST AI Risk Management Framework (AI RMF), including policies and procedures addressing AI system trustworthiness, accountability, and responsible AI development and deployment.

14.1.2. Core Functions. Provider's AI governance program addresses the four core functions of the NIST AI RMF:

14.1.2.1. **Govern.** Establishing organizational policies, procedures, and governance structures for responsible AI;

14.1.2.2. **Map.** Identifying and documenting AI system characteristics, potential impacts, and risks;

14.1.2.3. **Measure.** Implementing testing, evaluation, validation, and verification (TEVV) processes;

14.1.2.4. **Manage.** Implementing risk mitigation measures and continuous improvement processes.

14.1.3. Documentation. Upon reasonable request and subject to confidentiality obligations, Provider will provide Customer with high-level information regarding Provider's AI governance practices and alignment with the NIST AI RMF.

14.2. AI System Transparency.

14.2.1. System Information. Provider will provide Customer with reasonable information about the AI Systems integrated into the Services, including:

14.2.1.1. General description of AI capabilities and intended use cases;

14.2.1.2. Known limitations of the AI Systems;

14.2.1.3. General information about the types of data used to train or fine-tune AI models (without disclosing proprietary training data or methodologies);

14.2.1.4. Guidance on appropriate use cases and human oversight requirements.

14.2.2. Model Documentation. Provider maintains internal documentation of AI models, including versioning, training data characteristics, performance metrics, and known limitations. Summaries of such documentation may be provided to Customer upon request, subject to Provider's confidentiality requirements.

14.2.3. Output Attribution. Where technically feasible, Provider will provide indicators distinguishing AI-generated outputs from other content within the Services.

14.3. Bias Mitigation and Fairness.

14.3.1. Bias Assessment. Provider conducts periodic assessments of AI Systems to identify potential biases, particularly biases that could result in discriminatory outcomes based on protected characteristics such as race, ethnicity, gender, age, disability, or national origin.

14.3.2. Mitigation Measures. Provider implements technical and procedural measures designed to mitigate identified biases, including:

14.3.2.1. Diverse and representative training data selection where feasible;

14.3.2.2. Testing AI Systems across different demographic groups;

14.3.2.3. Implementing fairness metrics and monitoring;

14.3.2.4. Refining models based on bias assessment results.

14.3.3. Limitations Disclosure. Provider acknowledges that complete elimination of bias in AI Systems is not technically feasible. Provider will disclose known bias risks and limitations in Documentation and will work cooperatively with Customer to address bias-related concerns.

14.3.4. Customer Responsibility. Customer acknowledges that it has responsibility for:

14.3.4.1. Implementing human review and oversight of AI System outputs, particularly for decisions affecting individuals' rights, health, safety, or access to services;

14.3.4.2. Conducting its own bias assessments appropriate to its specific use cases;

14.3.4.3. Implementing safeguards to prevent discriminatory outcomes in Customer's use of the Services.

14.4. Explainability.

14.4.1. Explanation Capabilities. Where technically feasible and appropriate to the AI System's architecture, Provider implements explainability features to help users understand how AI Systems generate outputs, which may include:

14.4.1.1. Confidence scores or indicators;

14.4.1.2. Identification of key factors influencing outputs;

14.4.1.3. General explanations of the AI System's decision-making logic.

14.4.2. Technical Limitations. Customer acknowledges that certain AI architectures, particularly deep learning models, have inherent limitations in explainability. Full transparency into model internals may not be feasible without compromising model effectiveness or Provider's intellectual property.

14.4.3. Documentation. Provider will document explainability capabilities and limitations in the Documentation and will provide reasonable assistance to help Customer understand AI System outputs.

14.5. AI System Monitoring and Improvement.

14.5.1. Performance Monitoring. Provider continuously monitors AI System performance, including:

14.5.1.1. Output quality and accuracy metrics;

14.5.1.2. Error rates and types of errors;

14.5.1.3. User feedback and incident reports;

14.5.1.4. Compliance with intended use cases.

14.5.2. Model Updates. Provider may update, retrain, or replace AI models to improve performance, address identified issues, mitigate biases, or comply with legal requirements. Provider will:

14.5.2.1. Use commercially reasonable efforts to ensure model updates do not materially degrade functionality;

14.5.2.2. Provide notice of significant model changes through Documentation updates or Customer communications;

14.5.2.3. Maintain version control and change logs for AI models.

14.5.3. Feedback Mechanism: Customer may report AI System issues, errors, or concerns through Provider's support channels. Provider will investigate reported issues and implement appropriate remedial measures.

14.6. Human Oversight Requirements.

14.6.1. Human-in-the-Loop. Customer acknowledges that AI System outputs should be subject to appropriate human oversight, particularly for:

14.6.1.1. High-stakes decisions affecting individuals' health, safety, legal status, or access to benefits or services;

14.6.1.2. Decisions that may have significant legal, regulatory, or ethical implications;

14.6.1.3. Situations where AI System outputs contradict human expertise or common sense.

14.6.2. Decision Authority. Customer retains ultimate decision-making authority and responsibility for actions taken based on AI System outputs. AI Systems are designed to augment, not replace, human judgment.

14.6.3. Training Requirements. Customer is responsible for ensuring that Authorized Users receive adequate training on:

14.6.3.1. Appropriate use of AI System features;

14.6.3.2. Limitations and potential biases of AI Systems;

14.6.3.3. When human oversight and review are required;

14.6.3.4. How to identify and report AI System errors or concerns.

14.7. AI-Specific Security and Safety.

14.7.1. Adversarial Protections. Provider implements security measures designed to protect AI Systems against adversarial attacks, including:

14.7.1.1. Input validation and sanitization;

14.7.1.2. Rate limiting and abuse detection;

14.7.1.3. Monitoring for anomalous usage patterns;

14.7.1.4. Regular security testing of AI System components.

14.7.2. Safety Guardrails. Provider implements safety measures designed to prevent harmful outputs, including:

14.7.2.1. Content filtering for prohibited or harmful content;

14.7.2.2. Output validation checks;

14.7.2.3. Circuit breakers to halt operations in case of detected anomalies;

14.7.2.4. Mechanisms to detect and prevent prompt injection attacks.

14.7.3. Incident Response: AI-related security or safety incidents are subject to the incident response procedures in Section 6.7, with additional considerations for:

14.7.3.1. Assessing whether AI System outputs caused or contributed to harm;

14.7.3.2. Determining whether model retraining or updates are necessary;

14.7.3.3. Implementing corrective measures to prevent recurrence.

14.8. AI Regulatory Compliance.

14.8.1. Compliance Commitment: Provider will use commercially reasonable efforts to maintain compliance with applicable AI-related laws and regulations, including:

14.8.1.1. Federal AI regulations and executive orders;

14.8.1.2. State AI laws applicable to Provider's operations;

14.8.1.3. Industry-specific AI regulations (e.g., healthcare AI regulations).

14.9. Regulatory Changes: If new AI-related laws or regulations materially affect Provider's ability to provide the Services, Provider will:

14.9.1.1. Promptly notify Customer of such regulatory changes;

14.9.1.2. Work cooperatively with Customer to implement necessary changes to maintain compliance;

14.9.1.3. Modify the Services as necessary to achieve compliance, provided such modifications do not materially reduce functionality.

14.10. Customer Compliance: Customer is responsible for ensuring its use of the Services complies with all AI-related laws and regulations applicable to Customer's operations and jurisdiction.

14.11. Prohibited AI Uses. Customer shall not use the AI Systems or Services to:

14.11.1. Make automated decisions that have legal or similarly significant effects concerning individuals without appropriate human review and oversight;

14.11.2. Develop or train competing AI models or products;

14.11.3. Deliberately attempt to reverse engineer AI model architectures or training data;

14.11.4. Generate content intended to deceive, defraud, or harm individuals or organizations;

14.11.5. Violate individuals' civil rights or engage in unlawful discrimination;

14.11.6. Process data for surveillance purposes in violation of applicable law;

14.11.7. Generate content that violates applicable laws or regulations;

14.11.8. Any other use prohibited by applicable law or regulation.

14.12. AI Warranties and Disclaimers.

14.12.1. AI-Specific Warranties. Provider warrants that:

14.12.1.1. It has implemented reasonable AI governance practices designed to align with the NIST AI RMF;

14.12.1.2. It conducts periodic bias assessments and implements reasonable mitigation measures;

14.12.1.3. It maintains security measures designed to protect against known AI-specific vulnerabilities and attacks.

14.12.2. AI System Limitations: CUSTOMER ACKNOWLEDGES AND AGREES THAT:

14.12.2.1. AI SYSTEMS ARE PROBABILISTIC AND MAY PRODUCE INCORRECT, INCOMPLETE, BIASED, OR UNEXPECTED OUTPUTS;

14.12.2.2. PROVIDER DOES NOT WARRANT THAT AI SYSTEMS WILL BE ERROR-FREE, BIAS-FREE, OR WILL MEET CUSTOMER'S SPECIFIC REQUIREMENTS IN ALL CASES;

14.12.2.3. AI SYSTEM PERFORMANCE MAY VARY BASED ON INPUT DATA, USE CONTEXT, AND OTHER FACTORS;

14.12.2.4. CUSTOMER IS RESPONSIBLE FOR VALIDATING AI SYSTEM OUTPUTS AND IMPLEMENTING APPROPRIATE SAFEGUARDS FOR ITS SPECIFIC USE CASES.

14.13. AI-Related Incidents. Customer shall promptly notify Provider if Customer becomes aware of:

14.13.1. AI System outputs that appear to be significantly biased or discriminatory;

14.13.2. AI System errors that result in material harm or potential harm to individuals;

14.13.3. Apparent AI System security vulnerabilities or successful adversarial attacks;

14.13.4. Systematic patterns of AI System malfunction or poor performance.

Upon receipt of such notice, Provider shall investigate the reported issue and implement appropriate corrective measures in accordance with Section 6.7.