



AYBIL AGRICULTURAL TECHNOLOGIES

MASTER SERVICES AGREEMENT

Enterprise AI & Agricultural Intelligence Services

Version 1.0 | September 2026

Designed for institutional, enterprise and public-sector engagements

Document Status & Contracting Framework

This Master Services Agreement (the “MSA”) establishes the baseline legal and commercial framework under which Aybil Agricultural Technologies, operating the Umay Ana agricultural intelligence platform (“Provider”), may provide enterprise software, artificial-intelligence-enabled agricultural analytics, institutional data services, application access, APIs, dashboards, advisory workflows and related professional services to a customer identified in an applicable Order Form (“Customer”).

IMPORTANT: This document is a commercial contracting template and is intended to demonstrate enterprise readiness. It should be reviewed and, where necessary, adapted by qualified legal counsel before execution in a specific jurisdiction or regulated transaction.

Contract Structure

- This MSA governs the general relationship between the parties.
- Each Order Form defines the specific services, users, geography, pricing, term, data scope and implementation assumptions for an engagement.
- A Data Processing Addendum (“DPA”), security schedule, service-level schedule or project-specific statement of work may be incorporated by reference where required.
- In the event of conflict, the order of precedence is: (1) signed Order Form or Statement of Work, (2) DPA for privacy-specific matters, (3) applicable service or security schedule, and (4) this MSA, unless expressly stated otherwise.

Enterprise Positioning

Umay Ana is designed as an agricultural decision-support and risk-intelligence layer for farmers and for institutions serving agricultural populations. Depending on the applicable Order Form, services may include end-user application access, structured agricultural signals, weather- and location-aware analysis, crop and livestock support, sustainability evidence records, carbon-diary workflows, regenerative-agriculture guidance, institutional dashboards, portfolio views, controlled exports and APIs.

The parties acknowledge that certain outputs are probabilistic, inferential, AI-generated, derived from third-party data, or dependent on the quality and completeness of information supplied by users or external data providers. Accordingly, this MSA establishes clear boundaries for decision use, data responsibility and regulated workflows.

Table of Contents

Section	Subject
1	Definitions
2	Agreement Formation and Order Forms
3	Services and Implementation
4	Enterprise Licensing and Authorized Use
5	Customer Data, Platform Data and Data Rights
6	AI Systems, Analytical Outputs and Decision Boundaries
7	Data Protection, Privacy and Security
8	Confidentiality
9	Intellectual Property and Feedback
10	Fees, Invoicing and Taxes
11	Warranties, Compliance and Disclaimers
12	Indemnification
13	Limitation of Liability
14	Term, Suspension and Termination
15	General Provisions
Schedule A	Service Levels and Support
Schedule B	Security & Data Protection Summary
Schedule C	Enterprise Order Form Template
Schedule D	Signature / Acceptance Page

1. Definitions

“Affiliate”. an entity that directly or indirectly controls, is controlled by, or is under common control with a party.

“Aggregated Data”. data combined across multiple users, farms, records, customers, time periods or other sources in a manner intended not to identify an individual person or a specific Customer, subject to applicable law and agreed re-identification safeguards.

“AI Output”. any recommendation, classification, score, estimate, summary, generated text, risk indicator, forecast, trend, image interpretation, anomaly indicator or other result produced wholly or partly by machine-learning, generative-AI or statistical systems.

“Authorized User”. an employee, contractor, participating farmer, customer, insured, borrower, agent, official or other individual permitted by Customer and the applicable Order Form to use the Services.

“Customer Data”. data, content, records, images, files, identifiers or information submitted to the Services by or on behalf of Customer or its Authorized Users, excluding Provider technology, general product telemetry, and data lawfully obtained independently from Customer.

“Derived Signal”. a computed, normalized, inferred, scored or categorized signal generated from Customer Data, public information, licensed data, system telemetry or other authorized sources.

“Documentation”. Provider’s then-current user, integration, API, security or technical documentation made available for the Services.

“Personal Data”. information relating to an identified or identifiable natural person, or equivalent protected information under applicable data-protection law.

“Services”. the subscription services, APIs, dashboards, applications, analytical services, support, implementation or professional services stated in an Order Form.

“Usage Data”. technical and operational information about access to and operation of the Services, such as request volumes, feature usage, performance data, error logs, latency, device information and security events, excluding the substantive content of Customer Data except where technically necessary.

2. Agreement Formation and Order Forms

2.1 Scope. This MSA applies to every Order Form, Statement of Work or other ordering document that expressly incorporates it. No purchase order, procurement portal term or Customer form modifies this MSA unless Provider expressly agrees in a signed writing.

2.2 Order Forms. Each Order Form will identify, as applicable, the contracted modules, user or participant population, geographic scope, institutional use case, data categories, API or dashboard access, service period, fees, support level, implementation obligations and special compliance requirements.

2.3 Affiliates. An Affiliate may procure Services under this MSA by executing an Order Form. Unless otherwise stated, that Affiliate becomes the “Customer” solely for that Order Form and is responsible for its own obligations.

2.4 No Minimum Commitment. Unless an Order Form states otherwise, this MSA does not by itself require either party to purchase or deliver any minimum volume of Services.

2.5 Changes. Material changes to scope, population, data access, regulated use, integration or service level must be documented in a change order, amended Order Form or Statement of Work.

Recommended Institutional Order Model

For large deployments, the parties should separate the commercial population entitlement from technical consumption. For example, an institution may sponsor application access for an agreed portfolio of farmers while API, export, model-call, onboarding or premium-support volumes are separately measured and priced. This structure allows controlled scaling without treating every participant interaction as a separate contract.

3. Services and Implementation

3.1 Provision of Services. Provider will make the Services available in material accordance with the applicable Order Form and Documentation. Provider may use Affiliates, cloud providers, AI model providers, mapping providers, weather-data providers, communications providers and other subprocessors or subcontractors to operate the Services, subject to applicable confidentiality, security and data-protection obligations.

3.2 Implementation. Where implementation services are included, each party will provide timely personnel, access, information, decisions and technical cooperation reasonably required for onboarding, data mapping, API setup, testing, user communication and launch.

3.3 Customer Dependencies. Provider is not responsible for delay or degraded performance caused by Customer systems, unavailable third-party systems selected by Customer, inaccurate population lists, missing consents, defective credentials, blocked network access, unsupported devices or Customer's failure to meet agreed dependencies.

3.4 Changes to Services. Provider may improve, modify or replace features, models, user interfaces, workflows, infrastructure and third-party components, provided that Provider does not materially reduce the core functionality purchased for the then-current Order Form without a reasonable replacement or transition path.

3.5 Beta and Preview Features. Experimental, pilot, beta or preview features may be offered for evaluation. Unless expressly committed in an Order Form, such features are provided without service-level commitments and may be changed or withdrawn.

3.6 Professional Services. Deliverables from consulting, integration, analytics design, data mapping or other professional services will be described in a Statement of Work. Unless expressly stated otherwise, Provider retains ownership of pre-existing methods, templates, tools, software, know-how and reusable components used to create such deliverables.

4. Enterprise Licensing and Authorized Use

4.1 License Grant. Subject to payment and compliance with this Agreement, Provider grants Customer a limited, non-exclusive, non-transferable right during the applicable subscription term to access and use the Services for Customer's internal business, program, portfolio-management or public-service purposes described in the Order Form.

4.2 Sponsored End-User Access. Where Customer sponsors access for farmers, customers, policyholders, borrowers, beneficiaries or other participants, Provider may provision individual application access subject to agreed eligibility rules, fair-use limits, usage entitlements and applicable end-user notices or terms.

4.3 API and Export Use. Customer may use APIs, dashboards or exports only within the scopes, rate limits and purposes stated in the Order Form or Documentation. Customer must protect credentials, maintain least-privilege access, and promptly disable access for personnel who no longer require it.

4.4 Restrictions. Customer will not: (a) resell or sublicense the Services except as expressly authorized; (b) reverse engineer or attempt to derive non-public source code, model weights or system prompts except where restriction is prohibited by law; (c) circumvent usage limits or security controls; (d) use the Services to develop or train a directly competing product using unauthorized extraction of Provider outputs; (e) conduct harmful security testing without written authorization; or (f) use the Services unlawfully or in a manner that infringes third-party rights.

4.5 High-Risk Decisions. Unless expressly agreed in a regulated implementation, Customer will not use Umay Ana output as the sole basis for automatic approval, denial, pricing, payment, certification, claim settlement, credit underwriting, insurance eligibility, employment, legal status or other decision that produces material legal or similarly significant effects for an individual.

5. Customer Data, Platform Data and Data Rights

5.1 Customer Ownership. As between the parties, Customer retains all right, title and interest in Customer Data supplied by or on behalf of Customer, subject to the licenses necessary for Provider to perform the Services.

5.2 Processing License. Customer grants Provider and its authorized subprocessors a non-exclusive right to host, copy, transmit, normalize, validate, transform, analyze and otherwise process Customer Data solely to provide, secure, support and improve the Services; to comply with law; and for the additional purposes expressly permitted in this Section.

5.3 Aggregated and De-identified Use. To the extent permitted by applicable law and the applicable DPA, Provider may create and use Aggregated Data and data that has been reasonably de-identified so it is not intended to identify Customer or an individual. Provider may use such data for product improvement, benchmarking, model evaluation, model-risk testing, agricultural research, trend analysis, system performance, sustainability insights, portfolio-level analytics and development of generalized agricultural risk intelligence. Provider will not publicly disclose Aggregated Data in a manner that reasonably identifies Customer without Customer's permission.

5.4 Derived Signals. Unless an Order Form states otherwise, Customer may use Derived Signals delivered to it during the subscription for its authorized purposes. Provider retains ownership of the algorithms, schemas, taxonomies, feature engineering, scoring logic, model architecture and generalized methodologies used to generate such signals.

5.5 No Sale of Customer Personal Data. Provider will not sell Customer Personal Data to third parties for their independent advertising or unrelated commercial use. Any data sharing with subprocessors will be limited to the operation of the Services or another lawful, documented purpose.

5.6 Customer Responsibility for Source Legality. Customer represents that it has the rights, notices, permissions, legal basis and authority required to provide Customer Data to Provider and to instruct Provider to process it for the agreed institutional use case.

5.7 Data Return and Deletion. Upon expiration or termination, Provider will make Customer Data available for export for a commercially reasonable period if technically supported and requested, after which Provider may delete or anonymize it in accordance with its retention schedule, legal obligations, backup cycles and applicable DPA.

6. AI Systems, Analytical Outputs and Decision Boundaries

6.1 Nature of AI Outputs. The Services may use machine learning, generative AI, computer vision, statistical models, rules engines and third-party data. AI Outputs may be uncertain, incomplete, probabilistic or incorrect, and may vary as models, source data, weather conditions, agronomic context or user inputs change.

6.2 Decision Support. Unless expressly stated otherwise in an Order Form, AI Outputs are decision-support information, not a substitute for licensed agronomic, veterinary, financial, insurance, legal, medical, regulatory or other professional judgment.

6.3 Agricultural Context. Crop suitability, planting windows, irrigation, fertilizer timing, disease-risk indicators, livestock ration suggestions, sustainability practices and weather-related recommendations depend on local conditions and may require field verification, laboratory testing, soil analysis, veterinary review or local professional confirmation.

6.4 Institutional Risk Use. Portfolio views, credit-monitoring signals, claim-triage context, loss-prevention indicators, sustainability evidence, carbon-related records and other institutional outputs are intended to help prioritize review and improve information quality. They do not independently establish causation, legal liability, insurability, creditworthiness, carbon-credit issuance, regulatory compliance or entitlement to payment.

6.5 Human Oversight. Customer is responsible for establishing appropriate human review, escalation thresholds and governance for consequential uses of AI Outputs. Provider may provide confidence, provenance, coverage or evidence-status information where technically available, but Customer remains responsible for its final institutional decisions.

6.6 Model and Provider Changes. Provider may change model vendors, model versions, prompts, orchestration logic, validation methods and inference infrastructure as part of normal operation, provided that Provider continues to protect Customer Data in accordance with this Agreement and applicable DPA commitments.

6.7 No Training on Identifiable Customer Data Without Authorization. Provider will not intentionally use identifiable Customer Personal Data to train a general-purpose foundation model for unrelated third parties without Customer authorization or another lawful basis expressly permitted under the applicable DPA and law.

7. Data Protection, Privacy and Security

7.1 Compliance. Each party will comply with data-protection and privacy laws applicable to its own activities under this Agreement. Where Provider processes Personal Data on behalf of Customer as a processor or service provider, the parties will execute or incorporate an appropriate DPA.

7.2 Purpose Limitation and Data Minimization. The parties will define institutional purposes and select data fields reasonably necessary for those purposes. Customer should not request exact location, identity, images or other sensitive fields when aggregated, pseudonymous or lower-precision data is sufficient.

7.3 Security Program. Provider will maintain administrative, technical and organizational safeguards appropriate to the nature of the Services and risk, which may include access control, credential management, encryption in transit, environment separation, logging, backup practices, vulnerability management and incident-response procedures.

7.4 Security Incidents. Provider will notify Customer without undue delay after confirming a security incident involving Customer Data where notification is required by law or the applicable DPA, and will provide information reasonably available to support Customer's response obligations.

7.5 Subprocessors. Provider may appoint subprocessors. Where required by law or contract, Provider will maintain a subprocessor list or provide notice of material changes and will impose appropriate data-protection obligations on subprocessors that process Customer Personal Data.

7.6 International Transfers. Where Personal Data is transferred across jurisdictions, the parties will use legally recognized transfer mechanisms where required, which may include adequacy decisions, standard contractual clauses or other lawful safeguards.

7.7 Data Subject Requests. Where Provider acts as processor, Provider will provide reasonable assistance, taking into account the nature of processing and information available, for Customer to respond to lawful data-subject requests and regulatory obligations.

7.8 Sensitive Data. Customer will not provide special-category, highly sensitive or regulated personal information beyond what is necessary and agreed for the applicable use case. Health, biometric, financial-account, government-identifier or similar data should not be submitted unless expressly scoped and protected.

8. Confidentiality

8.1 Confidential Information. “Confidential Information” means non-public information disclosed by one party (“Discloser”) to the other (“Recipient”) that is marked confidential or that a reasonable person would understand to be confidential given its nature and context, including business plans, pricing, security information, source code, technical architecture, customer lists, agricultural datasets, model information and contractual terms.

8.2 Protection. Recipient will use Confidential Information only to perform or exercise rights under this Agreement and will protect it using at least reasonable care. Recipient may disclose Confidential Information only to personnel, Affiliates, professional advisers and subcontractors who need to know it and are bound by confidentiality obligations.

8.3 Exclusions. Confidential Information does not include information that Recipient can demonstrate: (a) is or becomes public without breach; (b) was lawfully known without restriction; (c) is lawfully received from a third party without confidentiality duty; or (d) is independently developed without use of the Discloser’s Confidential Information.

8.4 Compelled Disclosure. Recipient may disclose Confidential Information to the extent required by law, subpoena or court order, provided that Recipient gives advance notice where legally permitted and reasonable assistance to seek protective treatment.

8.5 Equitable Relief. Unauthorized disclosure of Confidential Information may cause irreparable harm for which monetary damages are inadequate. The Discloser may seek appropriate injunctive or equitable relief in addition to other remedies.

9. Intellectual Property and Feedback

9.1 Provider Technology. Provider and its licensors retain all right, title and interest in the Services, software, APIs, user interfaces, prompts, orchestration, model configurations, taxonomies, schemas, workflows, scoring methods, Documentation, designs, trademarks and all improvements and derivatives thereof, excluding Customer Data.

9.2 Customer Materials. Customer retains ownership of its trademarks, materials, proprietary datasets, documentation and other materials provided to Provider. Customer grants Provider a limited license to use them only to perform the Services and, where agreed, to identify Customer as a customer.

9.3 Feedback. If Customer provides ideas, suggestions or feedback regarding the Services, Provider may use them without restriction or obligation, provided that Provider does not disclose Customer Confidential Information in doing so.

9.4 Third-Party Components. Certain Services may incorporate third-party software, data or models subject to separate license terms or usage restrictions. Provider will identify material third-party restrictions where they materially affect Customer's permitted use.

9.5 Brand Use. Neither party may use the other party's name, logo or marks in public marketing without prior permission, except that Provider may include Customer in a factual customer list if the applicable Order Form expressly permits it. Public case studies require separate approval.

10. Fees, Invoicing and Taxes

10.1 Fees. Customer will pay the fees stated in each Order Form. Fees may be structured by subscription, sponsored participant, active user, API volume, analysis credit, data package, dashboard tier, implementation scope, support tier or another agreed metric.

10.2 Invoicing. Unless an Order Form states otherwise, recurring fees are invoiced in advance and professional services are invoiced according to milestones or monthly in arrears. Customer will pay undisputed invoices within thirty (30) days of invoice date.

10.3 Disputes. Customer must notify Provider of a good-faith invoice dispute before the due date or within a commercially reasonable period, identifying the disputed amount and basis. The parties will work promptly to resolve the issue. Undisputed amounts remain payable.

10.4 Taxes. Fees are exclusive of taxes, duties, levies and similar governmental charges. Customer is responsible for applicable indirect taxes, withholding taxes and transaction taxes, except taxes imposed on Provider's net income. If withholding is required by law, Customer will provide official evidence and cooperate in treaty relief where reasonably available.

10.5 Late Payment. Provider may charge legally permitted interest on overdue undisputed amounts and may suspend materially delinquent Services after reasonable notice, subject to applicable law and any agreed continuity protections for critical public-sector deployments.

10.6 Usage Overages. If Customer exceeds contracted volumes, Provider may charge agreed overage rates, request a revised Order Form, throttle non-critical excess usage, or agree a temporary capacity plan. Provider will not intentionally create surprise overage charges where usage alerts are reasonably available.

11. Warranties, Compliance and Disclaimers

11.1 Mutual Authority. Each party warrants that it has authority to enter into this Agreement and that the person executing an Order Form on its behalf is authorized to do so.

11.2 Service Warranty. Provider warrants that it will perform material professional services in a professional and workmanlike manner and will provide the subscription Services substantially in accordance with the applicable Documentation, subject to permitted maintenance and third-party dependencies.

11.3 Compliance. Each party will comply with applicable anti-bribery, anti-corruption, export-control, sanctions and trade laws in connection with this Agreement. Neither party is required to perform an obligation if doing so would violate applicable law.

11.4 Customer Use Compliance. Customer is responsible for determining whether its intended institutional use of AI Outputs, Personal Data, agricultural records, geolocation, sustainability evidence or financial/insurance workflows is lawful and appropriately governed in each jurisdiction of deployment.

11.5 Disclaimer. EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, THE SERVICES, AI OUTPUTS, THIRD-PARTY DATA AND BETA FEATURES ARE PROVIDED “AS IS” AND “AS AVAILABLE.” PROVIDER DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT AND ANY WARRANTY THAT AI OUTPUTS WILL BE ERROR-FREE, COMPLETE OR SUITABLE AS THE SOLE BASIS FOR A CONSEQUENTIAL DECISION, TO THE MAXIMUM EXTENT PERMITTED BY LAW.

11.6 External Conditions. Provider does not warrant weather, satellite, mapping, market, telecom, third-party model or external-data availability beyond Provider’s reasonable control. Agricultural outcomes are affected by local practices, climate, soil, disease, input quality, user behavior and other variables outside the Services.

12. Indemnification and 13. Limitation of Liability

12. Indemnification

12.1 Provider IP Indemnity. Provider will defend Customer against a third-party claim alleging that Customer's authorized use of the core Services infringes that third party's patent, copyright or trademark, and will pay damages finally awarded or settlement amounts approved by Provider, provided Customer gives prompt notice, reasonable cooperation and control of the defense to Provider.

12.2 IP Remedies. If an infringement claim is likely, Provider may procure the right to continue use, modify or replace the affected Service with materially equivalent functionality, or terminate the affected Service and refund prepaid fees for the unused portion of the term. This is Customer's exclusive remedy for covered infringement claims.

12.3 Exclusions. Provider has no indemnity obligation to the extent a claim arises from Customer Data, Customer modifications, combination with items not supplied or approved by Provider, use contrary to Documentation, or continued use after Provider provides a non-infringing replacement.

12.4 Customer Indemnity. Customer will defend Provider against third-party claims arising from Customer Data supplied without required rights, Customer's unlawful use of the Services, or Customer's use of AI Outputs as the sole basis for a prohibited consequential decision contrary to this Agreement, subject to equivalent defense procedures.

13. Limitation of Liability

13.1 Exclusion of Certain Damages. TO THE MAXIMUM EXTENT PERMITTED BY LAW, NEITHER PARTY WILL BE LIABLE FOR INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR FOR LOST PROFITS, LOST REVENUE, LOST BUSINESS, LOST GOODWILL OR LOSS OF DATA, ARISING FROM THIS AGREEMENT, EVEN IF ADVISED OF THE POSSIBILITY.

13.2 Liability Cap. EXCEPT FOR EXCLUDED CLAIMS BELOW, EACH PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATING TO AN ORDER FORM WILL NOT EXCEED THE FEES PAID OR PAYABLE UNDER THAT ORDER FORM DURING THE TWELVE (12) MONTHS PRECEDING THE EVENT GIVING RISE TO LIABILITY, OR, FOR AN ORDER FORM LESS THAN TWELVE MONTHS OLD, THE FEES COMMITTED FOR THE FIRST TWELVE MONTHS.

13.3 Excluded Claims. The limitations in Section 13.2 do not apply to liability that cannot lawfully be limited, fraud or willful misconduct, breach of confidentiality involving intentional disclosure, Customer's payment obligations, or indemnified third-party intellectual-property claims. A DPA may establish a separate negotiated cap for data-protection liability.

14. Term, Suspension and Termination

14.1 MSA Term. This MSA begins on the effective date of the first Order Form or signature and continues until terminated. Termination of this MSA does not automatically terminate an active Order Form unless the basis for termination applies to that Order Form.

14.2 Order Term. Each Order Form has the initial and renewal term stated in it. If silent, an Order Form does not automatically renew unless the parties agree in writing.

14.3 Termination for Cause. Either party may terminate an affected Order Form for material breach if the breach remains uncured thirty (30) days after written notice, or ten (10) days for undisputed non-payment. A party may terminate immediately for insolvency where permitted by law or for a material breach that cannot reasonably be cured.

14.4 Suspension. Provider may suspend access where reasonably necessary to prevent a security threat, unlawful activity, material harm to the Services, sanctions violation, misuse of credentials or persistent overdue payment. Provider will use reasonable efforts to limit the scope and duration and to notify Customer when lawful and practicable.

14.5 Effect of Termination. Upon termination, Customer's access rights end, outstanding undisputed fees become due, and each party will return or destroy the other party's Confidential Information as required, subject to lawful retention, backups and surviving obligations.

14.6 Survival. Sections concerning accrued payment, confidentiality, data rights that by nature survive, intellectual property, disclaimers, indemnification, liability, dispute provisions and other terms intended to survive will remain effective after termination.

15. General Provisions

15.1 Notices. Legal notices must be in writing and delivered by recognized courier, registered mail or email to the legal notice addresses specified in the applicable Order Form. Operational notices may be delivered through designated business or technical contacts.

15.2 Assignment. Neither party may assign this Agreement without the other party's prior written consent, not to be unreasonably withheld, except to an Affiliate or in connection with a merger, reorganization, sale of substantially all assets or change of control, provided the assignee is not a direct competitor where such restriction is lawful and assumes the obligations.

15.3 Independent Contractors. The parties are independent contractors. This Agreement does not create a partnership, joint venture, agency, employment, fiduciary or franchise relationship.

15.4 Force Majeure. Neither party is liable for failure caused by events beyond reasonable control, including natural disasters, war, civil unrest, government action, widespread telecom or cloud failure, epidemic, major cyberattack not caused by the affected party's failure to use reasonable safeguards, or failure of critical infrastructure, provided the affected party uses reasonable efforts to mitigate.

15.5 Governing Law. Unless an Order Form specifies another mutually agreed jurisdiction, this Agreement will be governed by the laws of the Republic of Türkiye, without regard to conflict-of-laws principles. The parties may agree in an Order Form to arbitration or courts appropriate to a cross-border institutional transaction.

15.6 Dispute Escalation. Before commencing formal proceedings, the parties will attempt in good faith to resolve a dispute through business escalation to designated senior representatives, except where urgent injunctive relief is reasonably required.

15.7 Entire Agreement. This Agreement and incorporated Order Forms and schedules constitute the entire agreement regarding their subject matter and supersede prior proposals or discussions on that subject. Amendments must be in writing and signed by authorized representatives.

15.8 Severability and Waiver. If a provision is unenforceable, it will be modified to the minimum extent necessary and the remainder will continue. Failure to enforce a provision is not a waiver.

15.9 Electronic Signatures. Electronic signatures, counterparts and electronic acceptance methods may be used to execute this Agreement and Order Forms to the extent permitted by law.

Schedule A - Service Levels and Support

This Schedule applies only where an Order Form states that production service levels are included. Pilot, beta and proof-of-concept environments are excluded unless expressly stated.

A.1 Availability Objective

Illustrative enterprise target: 99.5% monthly availability for agreed production API and institutional dashboard services, excluding scheduled maintenance, emergency maintenance, Customer-caused outages, internet or third-party failures outside Provider’s reasonable control, force majeure and suspended access permitted under the Agreement. A higher target may be negotiated for scaled deployments.

A.2 Incident Priorities

Priority	Example	Initial Response Target	Update Target
P1 Critical	Production unavailable or confirmed severe security impact	1 business hour or agreed 24x7 target	Every 2 hours while active
P2 High	Material degradation with no reasonable workaround	4 business hours	Daily or as agreed
P3 Normal	Non-critical defect or integration issue	1 business day	As progress changes
P4 Request	Question, enhancement or advisory request	2 business days	As appropriate

A.3 Maintenance and Status

Provider will use reasonable efforts to schedule material planned maintenance outside expected peak usage and to provide advance notice where practicable. Emergency security or infrastructure maintenance may occur without advance notice.

A.4 Service Credits

If negotiated in an Order Form, service credits are Customer’s sole financial remedy for a failure to meet an availability SLA and are calculated against the affected recurring service fee. No credit applies to excluded downtime. Credits must be requested within thirty (30) days after the affected month.

A.5 Support Model

Support may include designated contacts, onboarding, integration support, usage reviews, governance meetings, release communication and escalation paths. Premium 24x7 support is available only where expressly purchased.

Schedule B - Security & Data Protection Summary

B.1 Control Principles

- Least-privilege access and role-based administration for institutional services.
- Encryption in transit using industry-standard transport security; encryption at rest where supported by the underlying service architecture.
- Credential and secret management appropriate to production environments.
- Logging and traceability for institutional API requests, administrative actions and material security events where technically available.
- Segregation of production and development environments appropriate to the maturity and risk of the service.
- Regular dependency, vulnerability and patch management based on risk.
- Backup, recovery and business-continuity practices proportionate to contracted service criticality.
- Incident-response process with defined internal ownership and customer notification procedures.
- Subprocessor due diligence and contractual data-protection requirements appropriate to the service provided.
- Data-minimization, pseudonymization and purpose-scoped institutional exports where feasible.

B.2 Privacy Roles

The applicable Order Form and DPA should identify whether Provider acts as processor/service provider, independent controller, or both for different processing activities. End-user product analytics, account administration, fraud prevention and legally required security processing may involve separate roles from Customer-directed institutional processing.

B.3 Data Location and Transfers

Hosting location, subprocessors and cross-border transfer safeguards may vary by deployment and will be documented where required. Regulated customers may request a current subprocessor list and, where commercially feasible, region-specific hosting or data-residency options.

B.4 Retention

Retention periods should reflect the specific use case, legal basis, evidentiary need, contract term, dispute requirements, backup cycles and data-minimization principles. Exact retention commitments should be specified in the DPA or Order Form for regulated datasets.

Schedule C - Enterprise Order Form Template

Customer Legal Name	[Insert]
Customer Address	[Insert]
Provider	Aybil Agricultural Technologies / Umay Ana
Effective Date	[Insert]
Initial Term	[Insert]
Deployment Geography	[Countries / regions]
Institutional Use Case	[Banking / insurance / reinsurance / public sector / agribusiness / other]
Sponsored Population	[Eligible participants / farmers / users]
Modules	[App access / dashboard / API / analytics / sustainability / Carbon Diary / regenerative agriculture / other]
Data Scope	[Purpose-specific field set]
Integration	[API / export / SSO / dashboard / none]
Support Tier	[Standard / Premium / Custom]
Service Level	[Pilot / Production / Custom]
Fees	[Insert currency and pricing model]
Billing Schedule	[Insert]
Special Security / DPA Terms	[Insert or reference attachment]
Customer Contacts	Business: [] Technical: [] Security/Privacy: []
Provider Contacts	Business: [] Technical: [] Security/Privacy: []

Commercial and operational assumptions not expressly stated in this Order Form remain governed by the MSA. Any regulated decision workflow, automated action, use of sensitive Personal Data, or special data-residency requirement must be expressly documented before production use.

Schedule D - Signature / Acceptance Page

This Master Services Agreement may be executed together with an Order Form or may be incorporated by reference into an electronically accepted enterprise ordering process. The following signature blocks are provided for negotiated bilateral execution.

AYBIL AGRICULTURAL TECHNOLOGIES	CUSTOMER
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

UMAY ANA

Agricultural Vertical AI & Risk Intelligence

umay-ai.com