



UMAY ANA

SECURITY & TRUST OVERVIEW

Enterprise Security Architecture and Control Framework

Version 1.0 | September 2026

Enterprise AI & Agricultural Intelligence Services

Banks • Insurers • Reinsurers • Public Institutions • Agribusiness

Important drafting note. This overview describes the intended/current enterprise control framework without claiming certifications that have not been independently awarded. Customer-specific security commitments should be stated in the MSA, Order Form, DPA, or security schedule.

1. Security Principles

- Least privilege: grant only the access needed for a defined purpose.
- Defense in depth: combine application, infrastructure, identity, logging, and operational safeguards.
- Data minimization: expose only purpose-appropriate fields and precision.
- Traceability: preserve request, batch, or event identifiers where enterprise workflows require auditability.
- Human accountability: keep institutional users responsible for material decisions supported by AI outputs.
- Continuous improvement: adjust safeguards as product architecture, threats, and regulatory expectations evolve.

2. Data Governance and Segmentation

Umay Ana’s institutional design separates raw field observations, user-entered information, derived agricultural signals, and institutional outputs conceptually and, where applicable, through application- and database-level controls. Enterprise integrations are intended to use purpose-limited datasets rather than unrestricted data access.

Control area	Enterprise approach
Data classification	Differentiate customer-provided, self-recorded, system-derived, aggregated, and sensitive information.
Purpose limitation	Institutional APIs/exports should expose only fields needed for the contracted use case.
Location precision	Use the least precise geography sufficient for the use case where detailed coordinates are unnecessary.
Pseudonymous mapping	Partner subject references can be pseudonymous by default for institutional workflows.
Retention	Retention and deletion rules are aligned to service need, contract, law, backup, and security requirements.

3. Identity and Access Management

- Authenticated access to administrative and enterprise interfaces.
- Role-appropriate authorization and API scopes for institutional integrations.
- Credential and secret handling practices designed to prevent unauthorized disclosure.
- Access review and revocation processes proportionate to team size and operational risk.
- Customer responsibility for protecting its own credentials and promptly removing unauthorized users.

4. Encryption and Communications

Production web and API traffic is expected to use modern encrypted transport. Sensitive secrets should not be embedded in client-side code or shared through insecure channels. Encryption-at-rest controls depend on the underlying managed infrastructure and service configuration and may be documented in customer security questionnaires or contractual schedules.

5. Application and Infrastructure Security

- Environment separation and restricted production administration where practicable.
- Dependency and vulnerability management appropriate to the technology stack.
- Rate limiting, authentication checks, input validation, and abuse controls for externally exposed endpoints.
- Backup and recovery processes for critical production components.
- Change management proportionate to release risk, including review/testing before material production changes.

6. Logging, Monitoring and Traceability

Provider designs enterprise workflows to support operational logs and traceability without unnecessarily retaining sensitive payloads. Institutional responses or export batches may carry request/batch identifiers. Security and operational telemetry may be retained separately from customer-facing data to support incident response, reliability, and fraud prevention.

7. Security Incident Management

1. Identify and triage suspected security events.
2. Contain affected systems or credentials where appropriate.
3. Investigate scope and impact using available logs and evidence.
4. Remediate vulnerabilities or configuration issues.
5. Notify affected enterprise customers as required by contract and law.
6. Conduct post-incident review for material events and track corrective actions.

8. Third-Party and Subprocessor Risk

Umay Ana may rely on managed cloud, database, AI, messaging, analytics, or other technology providers. Provider evaluates third-party use based on function, data sensitivity, operational dependency, contractual protections, and available security information. Material Processors of Customer Personal Data are addressed through the DPA and applicable Subprocessor process.

9. AI and Model Security

- Treat user content and enterprise data as inputs subject to access and purpose controls.
- Avoid exposing confidential system prompts, credentials, or unnecessary personal information to model providers.
- Use structured outputs, validation, and application-side rules where practical for higher-impact workflows.

- Maintain a clear distinction between AI-generated advisory signals and authoritative legal, credit, insurance, certification, or agronomic determinations.
- Reserve the ability to change model providers or models to improve security, performance, cost, or quality, subject to contractual commitments.

10. Assurance and Customer Due Diligence

Provider supports reasonable enterprise due diligence through security questionnaires, architecture discussions, DPA/SLA review, and evidence that can be shared without compromising security. Umay Ana should not be represented as ISO 27001, SOC 2, PCI DSS, or another independently certified system unless and until the relevant certification or report has actually been obtained and remains current.

11. Shared Responsibility

Provider	Customer
Secure and operate contracted Provider-controlled services.	Secure Customer-controlled endpoints, devices, networks, user accounts, and integrations.
Provide access controls and enterprise integration mechanisms.	Assign appropriate users and protect credentials.
Respond to Provider-side incidents.	Notify Provider promptly about suspected misuse or compromised credentials.
Protect Customer data according to contract and law.	Ensure lawful basis, notices/consents, and appropriate source-data quality for Customer-provided information.

Acceptance and Relationship to the MSA

This document forms part of the Umay Ana enterprise contracting framework when incorporated by reference into a Master Services Agreement, Order Form, Statement of Work, or other written agreement executed by the parties. If there is a conflict, the order of precedence stated in the applicable agreement or Order Form will apply.

This template is intended to support commercial contracting and enterprise readiness. It should be reviewed by qualified counsel for the governing jurisdiction, the customer's regulatory status, data flows, and negotiated risk allocation before signature or public reliance.