MS Solutions E.A.S.

COMPLIANCE PROGRAM · VERSION 1.0

Compliance Manual — MS Solutions E.A.S.

AML/CFT Policy · Compliance Policy · Code of Ethical Conduct

ISSUED BY	MS Solutions E.A.S. — RUC 80171221-1 Gral. José de San Martín, Asunción, Paraguay
VERSION	1.0 · MSS-POL-01 · MSS-POL-02 · MSS-COD-01
APPROVED	May 5, 2026
NEXT REVIEW	May 2027
COMPLIANCE OFFICER	Maicon Guira (primary) · Suzana Nunes (deputy)
SCOPE	Entire organization
CLASSIFICATION	Public

Contents

MSS-POL-01

Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing Policy

How we identify our clients, assess the risk of each business relationship, and act when an operation is unusual or suspicious.

01 Purpose

This Policy sets out the principles, controls and procedures that **MS Solutions E.A.S.** applies to prevent, detect and manage the risk that its products, services, collection channels or infrastructure be used for **money laundering (ML)**, **terrorist financing (TF)** or the **financing of the proliferation of weapons of mass destruction (PF)**.

Its aim is to protect the integrity of the Company, of its clients and of its financial counterparties, and to ensure that the Company is not used — not even unwittingly — as a vehicle for illicit operations.

02 Scope

This Policy is binding on:

- The **partners and Management** of the Company.
- **All employees and contributors**, regardless of the form of their engagement.
- **Suppliers, contractors and business partners** acting on behalf of or in the name of the Company, to the extent relevant to their contractual relationship.

It covers every line of the Company's activity: infrastructure (dedicated and GPU servers), development and operation of its own SaaS platforms (Enplazo, En Regla and FacilitaPY), custom development, B2B solutions and applied artificial intelligence; as well as every channel through which the Company receives revenue.

03 Management statement

> The Management of MS Solutions E.A.S. declares its express and non-delegable commitment to the prevention of money laundering, terrorist financing and proliferation financing. No commercial target, business opportunity or client relationship justifies departing from this Policy. Management provides the resources required for its execution and upholds the independence of the Compliance Officer in the exercise of their duties.

04 Reference regulatory framework

The Company takes as its reference the following regulatory framework of the República del Paraguay and the applicable international standards:

- `Ley N° 1015/1997`, on the prevention and repression of acts intended to legitimise money or assets, as amended by `Ley N° 3783/2009` and `Ley N° 6497/2019`.
- `Ley N° 4024/2010`, punishing the criminal offences of terrorism, terrorist association and terrorist financing, as amended by `Ley N° 6408/2019`.
- `Ley N° 6419/2019`, regulating the freezing of financial assets of persons linked to terrorism and to the proliferation of weapons of mass destruction, and the procedures for the dissemination of, inclusion in and removal from sanctions lists issued pursuant to United Nations Security Council resolutions.
- `Ley N° 6446/2019`, creating the Administrative Registry of Legal Persons and Structures and the Administrative Registry of Beneficial Owners of Paraguay, and its implementing `Decreto N° 3241/2020`.
- Regulations issued by the **Secretaría de Prevención de Lavado de Dinero o Bienes (SEPRELAD)**, in its capacity as the Financial Intelligence Unit of Paraguay.
- The **FATF 40 Recommendations** and GAFILAT guidance, in particular Recommendations 1 (risk-based approach), 10 (customer due diligence), 11 (record keeping), 12 (politically exposed persons) and 20 (reporting of suspicious transactions).
- International financial sanctions regimes whose observance is required of the Company's counterparties, including the lists of the **United Nations Security Council** and of **OFAC** of the United States Department of the Treasury.

05 The Company's standing under Ley N° 1015/1997

MS Solutions E.A.S. is a technology company incorporated in Paraguay as an *Empresa por Acciones Simplificadas*, registered under `RUC 80171221-1`, with its registered office at Gral. José de San Martín, Asunción, Paraguay.

Given its corporate purpose and activity, the Company **does not carry out financial intermediation, does not administer third-party funds, and does not operate as a currency exchange, a remittance business, a payment processor or a virtual asset service provider**. It is therefore **not included in the list of obliged entities** under article 13 of `Ley N° 1015/1997`, nor has it been designated as such by SEPRELAD regulation.

Notwithstanding the above, the Company **voluntarily adopts** this prevention program, with the breadth and depth appropriate to its risk profile, for three reasons: (i) it operates with payment processors and financial institutions that are obliged entities and that legitimately expect an equivalent standard from their clients; (ii) it serves clients across several jurisdictions; and (iii) it regards the prevention of financial crime as part of its duty of care as a business.

The Company **cooperates fully** with the competent authorities and with its financial counterparties, and responds to their requests for information within the deadlines set and in accordance with applicable law.

06 Definitions

TERM	WORKING DEFINITION
Money laundering	Operations designed to conceal or disguise the illicit origin of assets or money, or to give them the appearance of legitimacy.
Terrorist financing	The provision or collection of funds or assets, by any means, with the intention that they be used for terrorist acts or by terrorist organisations or individuals.
Proliferation financing	The provision of funds or financial services for the manufacture, acquisition, development, transport or transfer of nuclear, chemical or biological weapons.
Client	Any natural or legal person with whom the Company holds, or intends to hold, a contractual relationship for consideration.
Beneficial owner	The natural person who ultimately owns or controls the client, or on whose behalf a transaction is conducted.
PEP	Politically Exposed Person: someone who holds or has held a prominent public function, together with their immediate family members and close associates.
Unusual operation	An operation inconsistent with the client's declared profile or lacking apparent economic rationale.
Suspicious operation	An unusual operation which, once analysed, gives reasonable grounds to presume a link to ML, TF or PF.

07 Program governance

Compliance Officer

Management appoints a **primary Compliance Officer** and a **deputy**, with unrestricted access to all Company information and a direct reporting line to Management:

ROLE	APPOINTEE	CONTACT
Compliance Officer (primary)	Maicon Guira — Technical Direction	contacto@mssolutionseas.com
Compliance Officer (deputy)	Suzana Nunes — Frontend · UX/UI · Quality Assurance	contacto@mssolutionseas.com

The deputy assumes the full set of duties in the event of the primary officer's absence, impediment or conflict of interest.

Duties of the Compliance Officer

1. Execute, maintain and update the AML/CFT/CPF program.
2. Approve the onboarding of clients rated **high risk** and decide on the refusal or termination of business relationships on compliance grounds.
3. Analyse escalated alerts, document the decision reached, and retain the corresponding file.
4. Respond to requests from competent authorities, financial institutions and payment processors.

5. Deliver the annual training plan.
6. Submit an **annual report** to Management on the operation of the program, the alerts handled and the improvements proposed.

The Compliance Officer acts with **independent judgement**. A decision not to onboard, or to terminate, a business relationship on compliance grounds cannot be overturned on commercial grounds.

08 Risk-based approach

The Company applies a risk-based approach: the intensity of controls is proportionate to the risk identified in each relationship. The assessment considers four factors:

FACTOR	ELEMENTS ASSESSED
Client	Legal form, business activity, length of standing, transparency of ownership structure, PEP status, presence on sanctions lists or in adverse media.
Product or service	Low-value recurring SaaS subscription, dedicated or GPU server, custom development, high-value B2B contract.
Channel	Online sign-up with card payment, local bank transfer, international transfer, in-person contracting or via an intermediary.
Geography	Country of incorporation and of operation, origin of funds, and standing on lists of high-risk jurisdictions or those under increased FATF monitoring.

These factors combine into a three-tier rating:

TIER	TYPICAL PROFILE	APPLICABLE MEASURE
Low	Paraguayan client with an active RUC, low-value recurring SaaS subscription, card payment or local transfer in the client's own name.	Simplified due diligence.
Medium	Overseas client, dedicated infrastructure, or material annual amounts with no red flags.	Standard due diligence.
High	PEP or PEP-linked, opaque ownership structure, high-risk jurisdiction, annual amounts of USD 10.000 or more, or the presence of red flags.	Enhanced due diligence and express approval by the Compliance Officer.

09 Customer due diligence

The Company **does not establish or maintain anonymous or fictitiously named business relationships**. Before activating a service, and on an ongoing basis throughout the relationship, it identifies and verifies its client.

Minimum information required

CLIENT TYPE	DATA AND VERIFICATIONS
Paraguayan legal entity	Corporate name, RUC and verification of its validity and standing against the register of the Dirección Nacional de Ingresos Tributarios (DNIT); address; declared business activity; identification of the legal representative; identification of the beneficial owner where the risk warrants it, and evidence of registration in the Administrative Registry of Beneficial Owners where applicable.
Paraguayan natural person	Full name, national identity card number or RUC, address, occupation and a verifiable means of contact.
Overseas client	Name or corporate name, tax identification number in the country of residence, country of incorporation and of operation, business activity and, for legal entities, identification of those exercising effective control.

All information collected is processed in accordance with the Company's Privacy Policy and Paraguayan data protection law.

Enhanced due diligence

Enhanced measures apply where a relationship is rated high risk. Depending on the case, they include:

- Requesting corporate documentation and identification of the beneficial owner.
- Documented enquiry into the **source of funds** and the economic rationale of the engagement.
- Searches of public sources and media regarding the client and its controllers.
- **Express prior approval** by the Compliance Officer to begin or continue the relationship.
- Monitoring at increased frequency and review of the file at least annually.

Updating and ongoing due diligence

Files are reviewed and updated: for low-risk clients, upon any material change; for medium risk, every two years; for high risk, annually. Any significant change in the client's contractual or payment behaviour triggers an immediate reassessment of their risk rating.

10 Politically Exposed Persons (PEPs)

The Company establishes whether the client, its legal representative or its beneficial owner is a PEP, and whether they are an immediate family member or close associate of a PEP.

PEP status **does not in itself lead to refusal of the client**, but it automatically results in a high-risk rating, the application of enhanced due diligence, and prior approval by the Compliance Officer. That status persists for the duration of the public function and for a reasonable period thereafter.

11 Sanctions screening

The Company screens its clients, legal representatives, beneficial owners, suppliers and business partners against:

- The sanctions lists of the **United Nations Security Council**, including those relating to terrorism and to the proliferation of weapons of mass destruction, and those disseminated by SEPRELAD pursuant to `Ley N° 6419/2019`.
- The **SDN** list and other restrictive lists of OFAC of the United States of America.
- European Union and United Kingdom sanctions lists, where applicable to the transaction.

Screening is carried out **before the service is activated** and repeated upon any material update to the lists and upon changes in the client's ownership or control.

Upon a **confirmed true match**, the Company: (i) does not enter into the relationship, or suspends it immediately if already under way; (ii) refrains from dealing with any linked funds or assets; (iii) reports the matter without delay to the competent authority and to the financial institution or payment processor involved; and (iv) fully documents its actions.

12 Payment methods, collections and operating restrictions

It is the Company's policy to receive revenue **exclusively through traceable electronic means**, via regulated financial institutions and payment processors that apply their own know-your-customer procedures.

Accordingly, the Company establishes the following binding rules:

1. **Cash payments are not accepted** for amounts equal to or above Gs. 10.000.000. Cash collections below that ceiling are exceptional, evidenced by a named tax receipt and recorded in the client's file.
2. **Third-party payments are not accepted** where no substantiated link to the contracting client exists. The payer must be the contract holder or must document their relationship with them.
3. **Every collection is supported by an electronic tax receipt** issued in the name of the actual client of the transaction. The Company does not issue receipts in the name of persons outside the contractual relationship, nor for items not actually delivered.
4. **Refunds are always made to the same payment method and the same original payer**, for the amount actually received. Refunds to accounts, cards or payers other than those of the original payment are not processed.
5. **Virtual asset payments are not accepted** directly. Should that method be enabled in future, it will only be through registered and supervised virtual asset service providers.
6. **Overpayments are not accepted**, nor are client credit balances held for amounts or periods lacking commercial justification.
7. **Funds originating from sanctioned jurisdictions** or from jurisdictions subject to FATF calls for action are not accepted.

13 Monitoring and red flags

The Company monitors its clients' contractual and payment behaviour. The following, among others, are red flags that require escalation to the Compliance Officer:

- Refusal, unjustified delay, or provision of false information when identification data, RUC or beneficial owner details are requested.
- A request that the invoice be issued in the name of a person or company unconnected to the contracting party, or a request that no receipt be issued.
- Repeated payment attempts using **multiple cards held by different people**, or with cards declined on a recurring basis.
- High-value infrastructure orders accompanied by **manifest indifference to technical specifications**, price or delivery time.
- Advance payment of amounts disproportionate to the declared profile or need, followed by a cancellation and refund request.
- A refund requested to an account, card or holder other than the one that made the payment.
- Funds originating from jurisdictions unconnected to the client's domicile or operations.
- Splitting a single contract into multiple smaller payments without commercial reason.
- Use of the contracted infrastructure for illicit activity, detected through abuse reports, third-party complaints or technical monitoring (phishing, fraud, malware distribution, botnets).
- A client who insists on anonymity, declines meetings or interviews, or communicates solely through non-attributable channels.
- The client, its representative or its beneficial owner appearing on sanctions lists or in adverse media relating to financial crime.

14 Alert handling procedure

1. **Detection and escalation.** Anyone who detects a red flag must report it to the Compliance Officer **immediately and in writing**. It is not for the individual to judge whether the matter is material.
2. **Analysis.** The Compliance Officer gathers the background, requests from the client any clarification or documentation deemed necessary, and assesses the economic rationale of the transaction.
3. **Decision.** The case closes in one of three ways: *justified operation* (documented and filed), *unusual operation without sufficient grounds* (kept under enhanced monitoring), or *suspicious operation*.
4. **Action on a suspicious operation.** The Company suspends delivery of the service so far as legally possible, refrains from further dealings with the counterparty, and **reports the matter to the competent authority**, as well as to the financial institution or payment processor involved, extending full cooperation.
5. **Documentation.** Each case is documented in a file recording the background, the analysis performed, the decision reached, its rationale, the person responsible and the date.

The Company **also documents dismissed alerts**: the absence of a report must be as explicable as its existence.

15 Confidentiality and prohibition of tipping-off

Personnel are prohibited from informing the client, its representative or any third party that an operation has been analysed, escalated or reported to a competent authority. This prohibition survives the end of the employment or contractual relationship.

Information relating to compliance analysis is treated as **strictly confidential** and access is restricted to the Compliance Officer, the deputy and Management.

16 Record keeping

The Company retains, on media that guarantee integrity, availability and traceability:

- Identification files for clients, legal representatives and beneficial owners: at least **5 years** from the end of the business relationship.
- Records of transactions, collections, refunds and tax receipts: **10 years**, in accordance with Paraguayan tax and commercial regulation.
- Files on alerts, analyses and compliance decisions, and training records: at least **5 years** from creation.

Records are held in a condition that allows a request from a competent authority or a financial counterparty to be answered **within the deadline set**.

17 Training

Every member of the team receives AML/CFT/CPF training **on joining** the Company and, as a minimum, **once a year**. Training covers the regulatory framework, the red flags relevant to the Company's activity, the escalation procedure and the consequences of non-compliance. Attendance and content are documented.

18 Supplier and business partner due diligence

Before engaging material suppliers, resellers or business partners, the Company verifies their identity, legal existence and absence from sanctions lists. Contracts with third parties acting on the Company's behalf include compliance clauses and a right of immediate termination for breach.

19 Independent review and updating

The program is reviewed **at least annually**, and additionally upon material regulatory change, the introduction of new products, collection channels or markets, or the occurrence of an incident. The review assesses whether the risk matrix remains current, the effectiveness of controls and delivery of the training plan, and is documented in the annual report to Management.

20 Non-compliance

Breach of this Policy constitutes serious misconduct and triggers the disciplinary regime set out in the **Code of Ethical Conduct**, without prejudice to termination of the contractual relationship and to any civil or criminal action that may follow.

21 Effective date

This Policy was approved by the Management of MS Solutions E.A.S. and has been in force since **May 5, 2026**, as **version 1.0**. The next scheduled review is due in **May 2027**. The current version is permanently published at mssolutionseas.com/en/compliance/.

MSS-POL-02

Compliance Policy

The governance framework through which the Company identifies the regulation that applies to it, manages its compliance risks, and verifies that they are observed.

01 Purpose

This Policy defines the **Regulatory Compliance Program** of **MS Solutions E.A.S.**: its governance, its components, the responsibilities assigned, and the control mechanisms through which the Company ensures that its operations conform to applicable law, to its contractual commitments and to its internal standards of conduct.

02 Scope

It applies to Management, to all employees and contributors, and to third parties acting on behalf of or in the name of the Company, across every line of activity and in every jurisdiction in which it operates or provides services.

03 Guiding principles

1. **Legality.** Compliance with the law is a condition of doing business, not a variable to be optimised.
2. **Integrity.** No commercial outcome justifies improper conduct.
3. **Proportionality.** Controls are sized to actual risk and to the size of the organisation, without becoming empty formality.
4. **Traceability.** Material decisions are documented; what is not recorded can be neither audited nor defended.
5. **Management accountability.** The commitment to compliance is declared and exercised from the top.
6. **Continuous improvement.** The program is reviewed periodically and corrected upon every deviation detected.

04 Applicable regulatory framework

The Company identifies and keeps current the body of rules governing its activity. As at this version, it principally comprises:

AREA	REFERENCE REGULATION
Corporate and commercial	Paraguayan Civil Code; `Ley N° 6480/2020` on *Empresas por Acciones Simplificadas*; `Ley N° 6446/2019` and `Decreto N° 3241/2020` on the Beneficial Owners Registry.

AREA	REFERENCE REGULATION
Tax	`Ley N° 6380/2019` on the modernisation and simplification of the national tax system; `Ley N° 6787/2021` creating the Dirección Nacional de Ingresos Tributarios (DNIT); the electronic invoicing regime and applicable general resolutions.
Employment and social security	`Ley N° 213/1993` — Labour Code, as amended; regulation of the Ministerio de Trabajo, Empleo y Seguridad Social (MTESS); the regime of the Instituto de Previsión Social (IPS).
Data protection	`Ley N° 7593/2025` on Personal Data Protection, enacted on November 27, 2025 and fully enforceable from November 2027; `Ley N° 1682/2001` and its amendments `N° 1969/2002` and `N° 6534/2020`; articles 33 and 36 of the National Constitution.
Consumer and e-commerce	`Ley N° 1334/1998` on Consumer and User Protection; `Ley N° 4868/2013` on Electronic Commerce.
Intellectual property	`Ley N° 1328/1998` on Copyright and Related Rights; `Ley N° 1294/1998` on Trademarks; third-party software licences and the open-source components used in its developments.
AML/CFT/CPF	`Ley N° 1015/1997` as amended; `Ley N° 4024/2010` and its amendment `Ley N° 6408/2019`; `Ley N° 6419/2019`; SEPRELAD regulations. Developed in the AML/CFT Policy.
Anti-corruption	`Ley N° 2523/2004`, preventing, defining and sanctioning illicit enrichment in public office and influence peddling; `Ley N° 977/1996` (Inter-American Convention against Corruption); `Ley N° 2535/2005` (United Nations Convention against Corruption). As it deals with counterparties in the United States, the Company additionally observes `FCPA` standards.
International sanctions	United Nations Security Council resolutions; OFAC restrictive lists and, where applicable, those of the European Union and the United Kingdom.

The Company performs a **regulatory review at least annually** and upon every material change in its activity, to incorporate new obligations and retire those that cease to apply.

05 Compliance governance

BODY	RESPONSIBILITY
Management	Approves the policies, allocates resources, sets the risk appetite and is ultimately accountable for the program.
Compliance Officer Maicon Guira (primary) Suzana Nunes (deputy)	Executes and maintains the program, assesses risks, runs the whistleblowing channel, delivers training, monitors and reports to Management. Acts with independent judgement.
Team	Know and apply the policies in their area of work, and report any deviation they become aware of without delay.
Third parties	Are contractually bound to observe the Company's standards to the extent relevant to their relationship.

Given the size of the organisation, the compliance function is performed by people who also hold operational roles. To preserve independence, the Company applies two safeguards: **(i)** no one approves a compliance case in which they have a direct interest — the deputy acts instead; and **(ii)** compliance decisions are documented in writing and made available to Management and to counterparties that legitimately request them.

06 Compliance risk management

The management cycle has four stages, performed and documented at least annually:

1. **Identification.** Mapping the applicable obligations and the processes capable of generating a breach.
2. **Assessment.** Estimating the likelihood and impact of each risk, including legal, financial, operational and reputational consequences.
3. **Treatment.** Defining preventive and detective controls, with an owner and a deadline.
4. **Monitoring.** Verifying control effectiveness and correcting the deviations detected.

07 Program components

The Compliance Program comprises the following documents, all publicly available and binding:

- **AML/CFT/CPF Policy** — know your customer, red flags and action on suspicious operations.
- **Code of Ethical Conduct** — expected conduct, conflicts of interest, whistleblowing channel and disciplinary regime.
- **Privacy Policy** — processing of personal data.
- **Cookie Policy** — storage technologies used on the site.
- **Terms and Conditions** — contractual framework of the services.

08 Anti-corruption and bribery

The Company applies a **zero-tolerance** policy towards corruption in any form. The following are expressly prohibited:

- Offering, promising, giving, requesting or accepting — directly or through third parties — money, gifts, favours or any benefit intended to obtain or retain business or an improper advantage.
- Making **facilitation payments**, even where of low value or customary in a given market.
- Using intermediaries, consultants or agents to channel improper payments.
- Making political contributions in the Company's name.
- Recording transactions inaccurately or incompletely, or creating unrecorded funds or accounts.

Any donation or sponsorship requires prior approval from Management, must have a documented legitimate purpose, and cannot be linked to obtaining business.

09 Dealings with public officials and bodies

The Company's platforms integrate technically with Paraguayan state bodies — among them the **DNIT**, the **IPS** and the **MTESS** — through official services, forms and channels. That integration is governed by the following rules:

- All interaction takes place **through the formal channels** made available by the body and in accordance with its terms of use.
- Client credentials for public systems are handled with the highest level of protection and used **solely** for the purposes authorised by the client.
- Offering any benefit to a public official in order to expedite, avoid or obtain a procedure, outcome or authorisation is prohibited.
- The Company does not represent that its products guarantee an outcome before a public body, nor does it suggest any influence over its decisions.

10 International sanctions and use of infrastructure

The Company supplies dedicated servers and GPU compute capacity. It therefore verifies that its clients are not subject to sanctions regimes and that the infrastructure contracted is not put to prohibited use.

Service contracts incorporate an **acceptable use policy** that expressly prohibits using the infrastructure for illicit activity — including fraud, phishing, malware distribution, attacks on third parties or infringement of intellectual property rights — and entitle the Company to **suspend the service immediately** upon breach, without any right to compensation.

11 Third-party due diligence

Before onboarding material suppliers, resellers or business partners, the Company verifies their identity and legal existence, their absence from sanctions lists and, where the risk warrants it, their public record. Contracts include compliance, data protection and confidentiality clauses, and a right of immediate termination for breach.

12 Data protection and information security

The Company operates platforms that process third parties' personal, tax and employment data. The specific commitments on processing, retention and the exercise of rights are set out in the Privacy Policy. From a compliance standpoint, the Company maintains:

- Encryption in transit using **TLS 1.2 or above** on all communications.
- Access control on a **least-privilege** basis, with individual credentials and periodic rotation.
- Logging of material events and continuous infrastructure monitoring.
- Backups and verified restoration procedures.
- An incident response procedure covering containment, analysis, notification of those affected and of the competent authority where applicable, and the adoption of corrective measures.

13 Responsible use of artificial intelligence

The Company embeds artificial intelligence components in its products. Their use is governed by the following commitments:

- **Human oversight.** Output generated by AI systems is supporting input; it replaces neither the user's professional judgement nor the Company's responsibility.
- **Transparency.** Users are told when they are interacting with an automated component.
- **Data protection.** Clients' personal or confidential data is not used for purposes other than delivering the contracted service.
- **Traceability.** Material decisions taken with AI support are logged and auditable.

14 Whistleblowing channel

The Company operates a channel for reporting regulatory breaches, conduct contrary to its policies, or indications of criminal activity. It is open to the team, clients, suppliers and any third party, at contacto@mssolutionseas.com, with the subject line **«Ética — Denuncia»**.

Anonymous reports are accepted. The Company guarantees the reporter's confidentiality and prohibits retaliation in any form. The operation of the channel is set out in the Code of Ethical Conduct.

15 Internal investigations

Every report or indication of a breach gives rise to an investigation led by the Compliance Officer, with guarantees of impartiality, confidentiality, the right to be heard and the presumption of innocence. Findings are documented and, where appropriate, result in disciplinary or corrective measures or in a report to the competent authority.

16 Training and communication

The Program documents are given to every member of the team on joining, together with an acknowledgement and acceptance record. Training is delivered **at least once a year** and upon every material update to the policies. Current versions are permanently published on the Company's website.

17 Monitoring and reporting

The Compliance Officer submits an **annual report** to Management covering, as a minimum: the outcome of the regulatory review, the updated risk matrix, the alerts and reports handled together with their outcome, delivery against the training plan, incidents recorded, and the improvement plan for the following period.

18 Non-compliance

Breach of this Policy, of the policies making up the Program, or of applicable regulation triggers the disciplinary regime of the **Code of Ethical Conduct**, without prejudice to termination of the relationship and to any legal action that may follow.

19 Effective date

This Policy was approved by the Management of MS Solutions E.A.S. and has been in force since **May 5, 2026**, as **version 1.0**. The next scheduled review is due in **May 2027**.

MSS-COD-01

Code of Ethical Conduct

What we expect of everyone who works at the Company or on its behalf: how we decide when nobody is watching.

01 Purpose

This Code brings together the principles and rules of conduct governing everyone connected with **MS Solutions E.A.S.**. It does not attempt to anticipate every possible situation: it sets the standard by which those not expressly covered are to be resolved.

> Where a situation is not covered by this Code, the question to answer is simple: **would this decision withstand being known by our client, our banking counterparty and the competent authority?** If the answer is no, the decision is wrong, however lawful or profitable it may be.

02 Scope

This Code binds the partners, Management, all employees and contributors — regardless of the form of their engagement — and third parties acting on behalf of or in the name of the Company. Knowing and accepting it is a condition of the relationship with the Company.

03 Our values

1. **Own what we do.** Every line of code, every server and every reply to a client has a named person responsible for it.
2. **Tell the client the truth.** Including when the truth is a mistake of ours, a deadline that will be missed, or a feature that does not exist.
3. **Comply with the law without exception.** It is not optimised, not conveniently interpreted, and not delegated to third parties.
4. **Guard other people's data as our own.** We handle third parties' tax, employment and personal information; protecting it is not negotiable.
5. **Compete on merit.** We win on product and service, never on improperly obtained information or by discrediting a competitor.

04 Compliance with the law

Everyone covered by this Code must know and comply with the regulation applicable to their role, as well as the Company's internal policies. Ignorance of an applicable rule does not excuse breaching it; in case of doubt, consult the Compliance Officer **before** acting.

05 Integrity in business

Corruption and bribery

Offering, promising, giving, requesting or accepting any improper benefit, directly or through third parties, in order to obtain or retain business or an advantage is prohibited. The prohibition covers both the public and private sectors and admits no exception for local custom, small value or urgency.

Gifts and hospitality

Customary business courtesies are permitted provided they meet all of the following conditions:

- Their value is reasonable and does not exceed the equivalent of **USD 100**.
- They are not cash or cash equivalents.
- They are neither offered nor received during a live tender, negotiation or procurement decision.
- They can be disclosed openly and recorded without discomfort.

Any courtesy exceeding that value, or coming from or directed to a public official, must be **declined** and reported to the Compliance Officer.

Conflicts of interest

A conflict of interest exists where a personal, family or financial interest may influence — or appear to influence — a decision taken on the Company's behalf. Typical situations include:

- Holding an interest in, or a connection with, a supplier, client or competitor of the Company.
- Engaging relatives or close associates, or taking part in decisions that benefit them.
- Outside professional activities that compete with the Company or that use its resources, information or time.
- Taking personal advantage of a business opportunity learned of by reason of one's role.

A conflict of interest is not in itself misconduct: **concealing it is**. Every actual or potential conflict must be declared in writing to the Compliance Officer as soon as it becomes known. Anyone affected by a conflict must abstain from the corresponding decision.

06 Fair competition

The Company competes on the quality of its products and services. Obtaining competitors' confidential information by unlawful or deceptive means, spreading false or disparaging statements about third parties, and entering into agreements that improperly restrict competition are all prohibited.

07 Dealings with clients

- Commercial, technical and contractual information given to a client must be **truthful, complete and verifiable**. We do not promise outcomes the Company cannot guarantee.

- Our own mistakes are communicated to the client **immediately**, together with their impact and the plan to fix them.
- Client data and credentials are used solely to deliver the contracted service.
- Any client request that would involve breaking the law is refused, including those involving irregular invoicing, concealment of information from public bodies, or misuse of third-party data.

08 Dealings with suppliers and partners

Suppliers are selected on objective criteria of quality, price, technical capability and regulatory compliance. No supplier is engaged because of a personal connection with the decision-maker. Suppliers are expected to meet a standard of conduct equivalent to this Code.

09 Dealings with authorities

The Company deals with public bodies through formal channels, submits truthful and complete information, and cooperates with legitimate requests from competent authorities. Offering any benefit to a public official is prohibited, as is suggesting to a client that the Company can influence a public decision.

10 AML/CFT in day-to-day conduct

Everyone must know the red flags set out in the AML/CFT Policy and report them to the Compliance Officer immediately and in writing. In particular, the following are prohibited:

- Accepting payments from people outside the contractual relationship.
- Issuing receipts in the name of someone who is not the actual client of the transaction, or for items not delivered.
- Processing refunds to an account or holder other than the one that made the payment.
- Telling a client or third party that an operation has been analysed, escalated or reported to an authority.

11 Confidentiality

Non-public information of the Company, its clients and its counterparties is confidential: source code, architecture, credentials, contracts, pricing, strategy, client data and personal information. The duty of confidentiality **survives indefinitely after the relationship** with the Company ends.

Extracting, copying or retaining Company information on personal devices, accounts or services without express authorisation is prohibited.

12 Protection of personal data

Personal data is processed in accordance with the Privacy Policy and applicable regulation. Each person accesses only the data their role requires, for as long as it requires it, and for the authorised

purpose. Accessing client data out of curiosity, personal interest or any purpose unrelated to the service constitutes **serious misconduct**.

13 Use of assets and systems

Equipment, licences, servers, accounts and credentials provided by the Company are working tools and must be used with care and for professional purposes. Sharing individual credentials, installing unlicensed software and circumventing established security controls are prohibited.

14 Ethical use of artificial intelligence

Anyone using artificial intelligence tools in their work must:

- **Verify** every output before passing it to a client or into a production system. Responsibility for the result always rests with the person, never with the tool.
- **Not enter** personal data, credentials or confidential client information into third-party services not authorised by the Company.
- **Not present** automatically generated content as professionally verified when it has not been.

15 Working environment

The Company maintains a respectful, safe working environment free of discrimination. All forms of harassment — workplace, sexual or of any other nature — are prohibited, as is discrimination on grounds of sex, gender identity or expression, sexual orientation, age, origin, nationality, religion, political opinion, disability, health status or any other characteristic.

Differences of view are raised directly and respectfully. Criticism is directed at decisions and work, never at the person.

16 Records and information

Every accounting, tax, technical or contractual record must reflect the reality of the transaction **accurately, completely and promptly**. Altering, destroying or concealing records is prohibited, as is creating documentation that does not reflect real events.

17 Public communications

Only expressly authorised people speak on the Company's behalf. In public statements and on social media, everyone must clearly distinguish their personal opinion from the Company's position, and refrain from disclosing confidential or client information.

18 Whistleblowing channel

Anyone — a member of the team, a client, a supplier or any third party — may report conduct contrary to this Code or to applicable regulation by writing to contacto@mssolutionseas.com with the subject

line **«Ética — Denuncia»**.

The Company undertakes the following:

- **Anonymous reports are accepted.** Identifying oneself is not a condition for a report to be handled.
- **Confidentiality.** The reporter's identity and the content of the report are handled in confidence and shared only with those who need to act on them.
- **No retaliation.** Retaliation against anyone who reports in good faith, or who assists an investigation, is in itself **serious misconduct**, regardless of whether the report is ultimately substantiated.
- **Acknowledgement and handling.** Every identified report is acknowledged within **5 business days**, and its outcome communicated to the reporter to the extent the confidentiality of the investigation allows.
- **Impartiality.** Nobody investigates a case in which they are involved or have an interest; in that event the deputy Compliance Officer, or Management directly, takes over.

A deliberately false report made in bad faith is also misconduct under this Code.

19 Consequences of breach

Breaches of this Code are assessed by reference to their seriousness, intent, the harm caused and the person's record, with the right to be heard guaranteed in every case. Measures may include:

SERIOUSNESS	MEASURE
Minor	Verbal or written warning and targeted training.
Serious	Formal reprimand on record, and review of access rights and responsibilities.
Very serious	Termination of the employment or contractual relationship, and report to the competent authority where the conduct may constitute a criminal offence.

The following, among others, are treated as **very serious**: corruption in any form, the deliberate compromise of clients' personal data, concealment of a suspicious operation, falsification of records, and retaliation against a reporter.

20 Acknowledgement and acceptance

Everyone receives this Code on joining and records in writing that they have read and accepted it. That record is renewed upon every material update to the document.

21 Effective date

This Code was approved by the Management of MS Solutions E.A.S. and has been in force since **May 5, 2026**, as **version 1.0**. The next scheduled review is due in **May 2027**.

Document approved by the Management of MS Solutions E.A.S. The current version is permanently published at mssolutionseas.com/en/compliance/. Any printed copy is considered uncontrolled.

Maicon Guira
primary · Dirección Técnica

Suzana Nunes
deputy · Frontend · UX/UI · Aseguramiento de la Calidad