MS SOLUTIONS E.A.S. · 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.

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

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

ROLE	APPOINTEE	CONTACT
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.

TIER	TYPICAL PROFILE	APPLICABLE MEASURE
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/.

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