MS SOLUTIONS E.A.S. · 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.

ISSUED BY	MS Solutions E.A.S. — RUC 80171221-1 Gral. José de San Martín, Asunción, Paraguay
VERSION	1.0 · MSS-POL-02
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 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.
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.

BODY	RESPONSIBILITY
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**.

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