INDEX

1. INTRODUCTION ..... .- 3 -
2. OBJECTIVE ..... .- 3 -
3. DEFINITION OF MONEY LAUNDERING ..... .- 3 -
4. REGULATORY AND SUPERVISORY AUTHORITIES ..... .- 4 -
5. PENALTIES ..... .- 5 -
6. AML/CFT REQUIREMENTS ..... .- 5 -
7. CUSTOMER IDENTIFICATION ..... .- 6 -
8. KNOW YOUR CUSTOMER (KYC) PROCESS ..... .- 6 -
KNOW YOUR SUPPLIER (KYS) AND KNOW YOUR PARTNER (KYP) PROCESSES ..... .- 7 -
9. KNOW YOUR EMPLOYEE (KYE) PROCESS ..... .- 7 -
10. EVALUATION OF NEW PRODUCTS AND SERVICES ..... .- 8 -
11. MONITORAMENTO DE TRANSAÇÕES ..... .- 8 -
12. TRANSACTION MONITORING ..... .- 9 -
13. TRAINING ..... .- 9 -
14. ROLES AND RESPONSIBILITIES ..... .- 9 -
14.1. COMPLIANCE AREA ..... .- 9 -
14.2. HUMAN RESOURCES AND LEGAL ..... .- 11 -
14.3. ALL AREAS OF GOWD ..... .- 11 -
14.4. MANAGEMENT AND EMPLOYEES ..... .- 11 -

1. INTRODUCTION

This document outlines the guidelines for Anti-Money Laundering and Counter-Terrorism Financing ("AML/CFT") and constitutes the AML/CFT Policy of GOWD TECNOLOGIA INSTITUIÇÃO DE PAGAMENTO ("GOWD"). This Policy was prepared based on current legislation and the regulations issued by the Central Bank of Brazil ("BACEN"), as well as market best practices. It aims to establish standards for the prevention and detection of money laundering or concealment of assets, rights, and values by the company's clients, its employees, or through the operations of the payment system.

2. OBJECTIVE

This Policy is an integral part of GOWD's governance structure and defines the procedures to be followed in the provision of services to our clients.

The main objectives of this Policy are:

• To establish principles, governance standards, and business practices to prevent GOWD from being used, directly or indirectly, as a money laundering mechanism; and

• To ensure that all GOWD employees are aware of the applicable rules and capable of carrying out the necessary procedures for preventing and combating money laundering and terrorism financing.

3. DEFINITION OF MONEY LAUNDERING

In Brazil, Law No. 9.613 of March 3, 1998 ("Law No. 9.613/98" or "Money Laundering Law"), in its Article 1, defines the crime of money laundering as concealing or disguising the nature, origin, location, disposition, movement, or ownership of assets, rights, or values derived, directly or indirectly, from a criminal offense.

Money laundering typically consists of distinct stages aimed at:

• Preventing transaction tracking;
• Breaking the link between the resources and criminal activities;
• Hiding the identity of those involved; and

• Returning the resources directly to the criminals or redirecting them for their benefit.

The money laundering process generally comprises the following stages, which may occur over time or simultaneously:

Placement – The insertion of illicit funds into the financial system through bank deposits, the purchase of negotiable instruments or goods, or transactions that accept cash.

Layering – The second stage involves making it difficult to trace the source of the funds by disrupting the audit trail. The perpetrator attempts to break the chain of evidence linking the funds to their criminal origin.

Integration – In this final stage, illicit resources are formally integrated into the economic system.

4. REGULATORY AND SUPERVISORY AUTHORITIES

The growing need for oversight and control has led to the expansion of official regulatory and supervisory bodies. These are national and international entities working to disseminate, regulate, and supervise the detection, prevention, and reporting of money laundering and related crimes.

In Brazil, the main regulatory and supervisory authorities are:

• Central Bank of Brazil (BACEN);
• Council for Financial Activities Control (COAF) – responsible for issuing regulations, imposing administrative penalties, receiving, examining, and identifying suspicious money laundering activities.

Internationally, the main regulatory and supervisory bodies are:

• OFAC;
• Vienna Convention;
• Financial Action Task Force on Money Laundering (FATF/GAFI);
• CICAD (Inter-American Drug Abuse Control Commission);
• Financial Intelligence Units (FIUs);
• Global Programme Against Money Laundering (GPML).

5. PENALTIES

Law No. 9.613/98 establishes severe penalties for individuals or entities that fail to comply with the required procedures for the prevention and combating of money laundering, both in criminal and administrative contexts.

Additionally, GOWD employees will be subject to internal disciplinary actions, including possible dismissal, in the event of failure to comply with any laws, regulations, or internal policies and procedures related to anti-money laundering and counter-terrorism financing.

Negligence and willful misconduct are considered violations of this policy and may lead to disciplinary measures by GOWD.

6. AML/CFT REQUIREMENTS

De To prevent money laundering and terrorism financing, and in compliance with legal and regulatory requirements applicable to GOWD, we implement the following procedures and internal controls:

- Customer Identification Process;
- KYC – Know Your Customer;
- KYP – Know Your Partner;
- KYS – Know Your Supplier;
- KYE – Know Your Employee;
- Evaluation of new products and services from an AML/CFT perspective;
- Monitoring customer behavior; and
- Employee training and awareness programs.

GOWD has a statutory director ("Director of Risk and Compliance") responsible for implementing and overseeing compliance with the rules and procedures established in this Policy, as outlined in section 15.1 below.

7. CUSTOMER IDENTIFICATION

This process involves a set of actions to identify customers, including collecting, updating, and storing registration data. It also includes specific procedures to:

a) Confirm customer identity using provided information and external sources. Required documents include the company's Articles of Incorporation, CNPJ registration, corporate structure, and a recent proof of address;

b) Identify ultimate beneficial owners and request identification documents for any individual holding more than 10% of the company's shares;

c) Identify customers classified as Politically Exposed Persons (PEPs) and assess whether a relationship can be established based on risk evaluation;

d) Prohibit relationships with individuals or entities listed on UN, OFAC, or EU financial sanctions lists or otherwise restricted by law.

8. KNOW YOUR CUSTOMER (KYC) PROCESS

This process comprises actions to obtain the identity, business activity, and the source and structure of the client's assets and financial resources. Customers presenting a higher money laundering risk must be subject to enhanced due diligence, with the approval of the Director of Risk and Compliance.

Accurate and timely information at the start of the relationship enhances the ability to identify money laundering risks.

The compliance department must receive and analyze complete onboarding information and documentation, approving or rejecting the continuation of the onboarding process.

Basic required documents include: a completed and signed onboarding questionnaire, articles of incorporation, proof of business address (within 90 days), a selfie of the managing partner holding an official ID and a dated note, bank statement, business license (if applicable), signed corporate structure, personal documents and proof of address (within 90 days) for all beneficial owners (over 10% shareholding), terms and conditions, privacy policy, AML/CFT policy, and compliance policy.

9. KNOW YOUR SUPPLIER (KYS) AND KNOW YOUR PARTNER (KYP) PROCESSES

The corporate procurement area follows procedures to identify, approve, and reassess suppliers, service providers, and partners, preventing contracts with unfit or potentially illicit entities. The key rule is to verify whether the supplier has any legal or operational restrictions.

10. KNOW YOUR EMPLOYEE (KYE) PROCESS

This includes rules, procedures, and controls for hiring and monitoring employees' financial backgrounds to avoid links with individuals involved in illicit activities.

11. EVALUATION OF NEW PRODUCTS AND SERVICES

New products and services must be assessed in advance from an AML/CFT perspective.

12. TRANSACTION MONITORING

Transactions by customers or end users must be monitored for signs of money laundering or terrorism financing. For high-risk cases—such as PEPs or clients flagged through GOWD's risk criteria—special measures include:

- Suspension of transactions pending additional verification;
- Termination of the relationship;
- Reporting to regulators;
- Other case-specific actions.

All users must have their CPF (individual taxpayer number) validated against Receita Federal's database (or another approved source if unavailable), with a maximum validity of 3 months per verification.

GOWD uses internal tools to automatically block transactions when a user reaches their assigned financial capacity limit, with further activity permitted only in subsequent periods or upon submission of lawful income proof.

Trained staff, supported by external tools, also perform ongoing transaction reviews to detect and prevent suspicious activity.

13. REPORTING SUSPICIOUS TRANSACTIONS

Transactions or proposals suspected of involving money laundering or terrorism financing must be reported to partners and applicable regulatory bodies in accordance with legal and regulatory requirements. Reports made in good faith do not result in civil or administrative liability for GOWD or its management and staff.

14. TRAINING

The AML/CFT training program is continuous and mandatory for eligible employees. Its objectives are to:

• Deepen employee understanding of legal and regulatory AML/CFT obligations and corporate guidelines;
• Equip staff to identify, prevent, manage, and report risks or signs of money laundering or terrorism financing.

Training may include in-person or online courses, webinars, conferences, awareness campaigns, and other formats.

All participants must sign a participation statement and pass an evaluation with a minimum score of 70%.

15. ROLES AND RESPONSIBILITIES

15.1. COMPLIANCE AREA

GOWD's Compliance area is responsible for implementing this Policy, evaluating suspicious activity, and deciding on reporting or internal actions. Responsibilities include:

a) Assessing suspicious cases and determining next steps, including partner or COAF notifications;
b) Implementing training programs at onboarding and on a periodic basis;
c) Continuously updating this Policy;
d) Ensuring compliance across all departments;
e) Defining GOWD's AML guidelines;

f) Assessing AML risks for new products and services;
g) Establishing criteria for client, supplier, and partner AML risk classification;
h) Supporting business areas in implementing AML processes;
i) Monitoring emerging typologies and recommending countermeasures;
j) Analyzing transactions for AML red flags and reporting to authorities as needed;
k) Evaluating staff-related suspicious activity and escalating to HR when necessary.

The Director of Risk and Compliance is further responsible for:

a) Ensuring documentation and records related to AML/CFT actions are kept as per regulation, for at least 5 years;
b) Keeping this Policy up to date;
c) Ensuring appropriate training is delivered to employees and collaborators in coordination with the Compliance area.

15.2. HUMAN RESOURCES AND LEGAL

These departments are responsible for applying KYE procedures, flagging complex issues to Compliance, analyzing AML legal and regulatory implications, supporting action plans, and assessing suspicious transactions from a legal standpoint.

15.3. ALL AREAS OF GOWD

They define and implement procedures and controls in compliance with the corporate guidelines for the prevention of money laundering and terrorism financing, in line with the complexity and risks associated with their respective processes.

They ensure that employees complete the required training on anti-money laundering (AML) and counter-terrorism financing (CTF).

They guarantee adherence to the corporate AML/CFT guidelines.

They monitor the money laundering risks and the corresponding controls within their respective area, under the direct supervision of the executive.

15.4. MANAGEMENT AND EMPLOYEES

All staff must understand and comply with this Policy, complete AML training, report any suspicious activity or proposal to the Compliance area, and respond promptly to Compliance inquiries regarding AML/CFT matters.