MRB INTERMEDIAÇÃO E NEGÓCIOS DIGITAIS	**Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Policy**	Code:	POL-RC-001
		Version No.:	1.0

Category:	Risks and Compliance	
Classification:	Last publication:	Next review:
Public	02/04/2024	30/03/2025

TABLE OF CONTENTS

1. TERMS AND DEFINITIONS

- **AML / CFT** – Anti-Money Laundering / Combating the Financing of Terrorism.
- **BACEN / BCB / BC** – Central Bank of Brazil.
- **Background check** – Process of verifying basic information and background of a person or entity, typically focused on criminal history, employment, and education, aiming to confirm the accuracy of provided information. It is simpler and more superficial than due diligence, primarily focused on verifying the truthfulness of previously provided information.
- **Board of Directors** – Managing Partner or Director appointed to represent Senior Management.
- **Brazilian Payment System (SPB)** – System managed by the Central Bank of Brazil (BCB) to enable operations and transfer of financial resources within the national territory, both in Brazilian reals and foreign currency. It consists of two segments: Financial Market Infrastructures (IMF) and Payment Arrangements.
- **Council for Financial Activities Control (COAF)** – Brazilian financial intelligence unit, established by Law No. 9,613/98, responsible for combating money laundering crimes by determining policies and guidelines to prevent illicit activities in the financial system.
- **Due diligence** – Comprehensive and detailed investigation of all relevant aspects of a person, company, or business, involving financial, legal, regulatory, and operational analysis, with the aim of identifying risks, opportunities, and critical issues before making strategic or financial decisions.
- **Employees** – Individuals working for the organization, including full-time, part-time, temporary, contracted, outsourced, and freelancers, including interns and apprentices.
- **Financial Action Task Force (FATF)** – Intergovernmental body aiming to develop and promote national and international policies to combat money laundering and terrorist financing.
- **Fraud** – Any illegal or illegitimate acts characterized by malicious deception, concealment, or violation of truth, regardless of the application of threat, violence, or physical force. Perpetrated by individuals and/or organizations to obtain money, goods, or services; avoid payment or loss of services; ensure personal or business advantage.
- **Improvement Opportunities** – Areas or processes that can be enhanced to increase efficiency, quality, or results.
- **Internal Risk Assessment (IRA)** – In accordance with BCB Circular No. 3,978/2020.
- **Know Your Client (KYC)** – Institutional rules and procedures adopted to identify and mitigate risks related to clients, during their accreditation and subsequently, aiming to understand their activities and effectively monitor their operations to prevent MRB's structure and/or products from being used as instruments for illicit activities.
- **Know Your Employee (KYE)** – Institutional rules and procedures to identify and mitigate risks related to employees, during their hiring and subsequently, to prevent MRB's structure from being used for illicit activities and other situations of conflicts of interest.
- **Know Your Partners (KYP)** – Institutional rules and procedures adopted to identify and mitigate risks related to business partners, assessing and legitimizing their reputation to avoid MRB's association with illegal activities.
- **Know Your Supplier (KYS)** – Institutional rules and procedures to examine the credibility and practices of suppliers to ensure ethical supply and reduce regulatory risks, preventing MRB's structure from being involved in illicit practices.
- **ML/TF** – Money Laundering / Financing of Terrorism.
- **MRB** – MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA, registered under CNPJ No. 38,354,463/0001-24.
- **National Financial System (SFN)** – Brazilian network of public and private institutions responsible for supervising and regulating operations in the Brazilian financial market.
- **Office of Foreign Assets Control (OFAC)** – Financial intelligence agency of the United States Department of the Treasury that monitors and updates the list of individuals and companies prohibited from doing business with the U.S. government and companies conducting business in the U.S., with extraterritorial reach.
- **Payment Institution** – Legal entity facilitating buying, selling, and movement of funds within a payment arrangement, without the ability to grant loans and financing to its customers, and whose main or ancillary

activity includes the options listed in article 6, item III, of Law No. 12,865 of October 9, 2013. They are not part of the SFN but are regulated and supervised by the BC, following guidelines established by the CMN.

- **Politically Exposed Person (PEP)** – Any public official with public exposure or person closely related to them, considering the verification of this condition as per article 27, as well as the condition of representative, family member, or close collaborator of these individuals as per article 19, both of Circular No. 3978/2020 of the BCB.
- **Risks and Compliance** – Department responsible for the governance, implementation, and monitoring of MRB's AML/CFT program, risk management, and regulatory compliance.
- **Securities and Exchange Commission (CVM)** – Regulatory body for the capital market in Brazil, responsible for regulating and overseeing companies and professionals operating in this market, aiming to protect investors and ensure market integrity.
- **Senior Management** – Partners and high-level executives responsible for defining strategies, making crucial decisions, and guiding the overall direction of the organization.

2. INTRODUCTION

In light of the growing landscape of financial threats, which encompasses not only traditional fraud and money laundering mechanisms but also concerns regarding the financing of terrorist activities, the implementation of this Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Policy is crucial for Payment Institutions in the country, compliant with the guidelines of the Central Bank of Brazil (BCB) and other regulatory requirements imposing rigorous standards of security and monitoring.

By investing in appropriate technologies and procedures to ensure legal compliance, MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA ("MRB") seeks not only to mitigate the risks associated with the subject matter but also to foster an organizational culture of integrity and transparency in its activities. This reinforces clients' trust in the payment institution, demonstrating its commitment to the security of data and financial transactions, in addition to strengthening the company's reputation and credibility in the market.

Ultimately, the implementation of this Policy serves to protect the interests of the institution while also contributing to the security, integrity, and stability of the Brazilian Payment System (SPB).

3. OBJECTIVE

Through this Policy, MRB aims to:

- Establish guidelines for the prevention, identification, and treatment of activities related to fraud and money laundering, including combating terrorism financing, considering MRB's risk profiles, its clients, operations, transactions, products, and services, as well as its employees, partners, and third-party service providers.
- Define the obligations and responsibilities of each area of the company on this matter.
- Ensure the adequacy, strengthening, and functioning of the internal control system.

4. SCOPE

This Policy applies to all individuals associated with MRB, including managers, investors, employees, interns, service providers, consultants, and any other natural or legal persons who utilize or support the Institution's Payment businesses.

5. NORMATIVE REFERENCES

- **Recommendations of the Financial Action Task Force - FATF**
- **Law No. 9,613, dated March 3, 1998** - Provides for the crimes of money laundering or concealment of assets, rights, and values; the prevention of the use of the financial system for the offenses provided for in this Law;

- **Law No. 12,865 of October 9, 2013** - Provides for payment arrangements and payment institutions that are part of the Brazilian Payment System (SPB).
- **Law No. 13,260, dated March 16, 2016** - Regulates item XLIII of Article 5 of the CF, disciplining terrorism, dealing with investigative and procedural provisions, and reformulating the concept of terrorist organization.
- **Circular No. 3,978 of January 23, 2020** - Provides for the policy, procedures, and internal controls to be adopted by institutions authorized to operate by the Central Bank of Brazil aimed at preventing the use of the financial system for the practice of money laundering or concealment of assets, rights, and values, as provided in Law No. 9,613/1998, and terrorism financing, as provided in Law No. 13,260/2016.
- **Circular Letter No. 4,001 of January 29, 2020** - Discloses a list of operations and situations that may indicate the occurrence of money laundering or concealment of assets, rights, and values, and Terrorism Financing, subject to reporting to COAF.
- **Coaf Resolution No. 40, dated November 22, 2021** – Provides for procedures to be observed regarding politically exposed persons, by those subject to the supervision of the Financial Activities Control Board (COAF).
- **BCB Resolution No. 80/2021** - Governs the establishment and operation of payment institutions, establishes the parameters for submitting requests for authorization to operate by these institutions, and provides for the provision of payment services by other institutions authorized to operate by the Central Bank of Brazil.
- **Joint Resolution No. 6 of May 23, 2023** - Provides for requirements for sharing data and information on fraud indicators to be observed by financial institutions, payment institutions, and other institutions authorized to operate by the Central Bank of Brazil.
- **BCB Resolution No. 343 of October 4, 2023** - Provides for the necessary measures for the execution of data and information sharing on fraud indicators as provided for in Joint Resolution No. 6, dated May 23, 2023.
- **Law 14,790/23 of December 29, 2023** - Allows private companies to operate online sports betting and in physical establishments, such as betting houses and casinos.

The laws and regulations are cited by way of example and do not exhaust all the applicable legislation to MRB's activities.

5.1. Applicability

MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA is a Payment Institution, founded in 2020, with the following corporate purpose: *"Execution or facilitation of payment activities related to a specific payment service, including transfers originated from or destined to digital payment accounts, services in the area of electronic payment means, auxiliary activities of financial services, intermediation and brokerage activities of services and businesses, except real estate, services provided on online payment platforms, digital wallets for making payments through electronic devices, commercial electronic solutions in the transmission, processing, and financial settlement with credit and debit cards, processing and settlement services for credit and debit card transactions, intermediation in obtaining loans."*

Thus, MRB will amend this Policy when necessary to:

- Comply with the entirety of the monitoring and selection procedures outlined in Circular No. 3,978/2020; and
- In the event of requesting authorization to operate from the Central Bank for the "Payment Institution" modality, in accordance with Law No. 12,865 of October 9, 2013, and BCB Resolution No. 80/2021. At

this point, MRB will also take the necessary steps to comply with Joint Resolution No. 6 of May 23, 2023, and BCB Resolution No. 343 of October 4, 2023, regarding the sharing of data and information on indicators of fraud.

6. GENERAL PROVISIONS

- The Senior Management of MRB commits to the effectiveness and continuous improvement of the policy, procedures, and internal controls related to AML/CFT, adopting, through its Risk and Compliance area, internal standards, norms, procedures, training, corporate communication, and preventive, corrective, and punitive measures, to ensure that the institution, in all areas, adheres to this Policy.
- Processes should be implemented to monitor the effectiveness and enhance this Policy and the means of preventing fraud risks.
- This policy should be understood in conjunction with other relevant institutional policies, and its content does not replace or override any legal instrument.
- Prior analysis of potential AML/CFT risks for new products and services, as well as the use of new technologies by MRB, must be conducted by the Risk and Compliance area. Parameters and best practices of Information Security established by the responsible area must also be adhered to.

7. CONCEPTS

7.1. Money Laundering

Money laundering, also known as *capital laundering*, is a criminal practice aimed at concealing the nature, origin, location, disposition, movement, or ownership of assets, rights, or values derived, directly or indirectly, from illicit acts or predicate crimes. Through this process, assets or resources obtained illegally are introduced into the formal economy, appearing to be legal, thereby hindering the identification and punishment of those responsible.

Money laundering is classified as a crime under Law No. 9,613/1998 and is punishable by imprisonment from 3 (three) to 10 (ten) years, a fine, and other sanctions.

There are three phases that characterize money laundering:

- PLACEMENT: This phase aims to place illicit assets or resources into the formal economy, meaning in legitimate companies or businesses. This phase involves the introduction of illicit assets or resources into the financial system, making it difficult to trace their origin.
- LAYERING: This involves taking measures to hinder the tracing of illicit assets or resources. During this phase, there's an attempt to conceal evidence and the connection between the asset and the committed crime. Various financial transactions may be conducted to add complexity and hinder future tracing.
- INTEGRATION: After being laundered and "cleaned" through different financial operations, the assets or resources return to the agents through the simulation of apparently legitimate businesses.

It is not necessary for all three phases of the offense to be present, as each phase, individually, is considered money laundering.

7.2. Terrorism Financing

Such financing is related to the disguised distribution of assets or resources to be used in acts and/or by terrorist organizations, as well as the financing of the proliferation of weapons of mass destruction. The methods used are generally similar to those employed in money laundering.

Law No. 13,260/2016 provides for the crime of financing in its article 6, imposing a penalty of imprisonment from 15 (fifteen) to 30 (thirty) years for anyone who *"receives, provides, offers, obtains, keeps in deposit, solicits, invests, in any way, directly or indirectly, resources, assets, goods, rights, values, or services of any kind, for the planning, preparation, or execution of crimes"* provided for in this Anti-Terrorism Law.

In the sole paragraph of the same legal provision, it states that *"the same penalty applies to anyone who offers or receives, obtains, keeps in deposit, solicits, invests, or in any way contributes to the obtaining of assets, goods, or financial resources, with the purpose of financing, totally or partially, a person, group of people, association, entity, criminal organization whose main or secondary activity, even on an occasional basis, is the practice of the crimes provided for in this Law"*.

8. ROLES AND RESPONSIBILITIES

Clear assignment of roles and responsibilities within AML/CFT is crucial to ensuring effective implementation of the Policy, as it helps ensure that all involved parties understand their specific functions and contribute to regulatory compliance and risk mitigation, enabling proper accountability. Thus, outlined below in a concise manner are the assignments of MRB's business areas:

8.1. Senior Management

- Ensure institutional adherence to AML/CFT best practices and compliance with relevant laws and regulations.
- Approve the development, revision, and changes to this Policy for subsequent publication.
- Designate and formally appoint, to the Central Bank of Brazil, a Director responsible for compliance with MRB's AML/CFT management obligations, in accordance with Circular BCB No. 3,978/2020.

8.2. Risk and Compliance

- Foster an organizational culture of anti-money laundering and counter-terrorism financing involving directors, clients, employees, suppliers, and business partners.
- Ensure compliance of business areas and all internal procedures of MRB.
- Create and manage control mechanisms aimed at AML/CFT prevention.
- Coordinate communication and training for Directors and Employees.
- Ensure compliance with the Reporting Channel's operating mechanisms.
- Monitor occurrences of suspicious or unusual transactions identified by MRB's technological tools or reported by Employees.
- PEP screening and monitoring, when necessary.
- Analysis of clients, suppliers, and other stakeholders involved in sanction lists.
- Communication with COAF and Bacen, as well as handling audits and other regulatory bodies and competent authorities.
- Effective corporate risk management.
- Effective communication of the Policy through institutional channels and training.
- Check for updates, revocation, and issuance of new regulations.

- Analyze potential AML/CFT risks for new products and services, as well as the use of new technologies by MRB.
- Conduct periodic Policy reviews.
- Analyze omissions or exceptions to what is established in this Policy (via the Board, as per item 20).
- Management of tools and establishment of processes related to background checks and due diligence.

8.3. Information Technology / Information Security

- Establish parameters and best practices for Information Security for MRB's products, services, and operations.
- Ensure full compliance with access restrictions to systems, electronic process approvals, rule parameterization changes in systems, and others, formalized and implemented by Access Management based on roles, Information Security Policy, and other necessary internal regulations and procedures.
- Test cybersecurity controls for fraud prevention.
- Diligently act to protect and maintain the confidentiality of data and MRB's technological tools and infrastructure.
- Monitor the security of all applications, systems, communication with suppliers, and MRB's technology structures to mitigate any risks of manipulation, cyberattacks, or exploitation of systemic vulnerabilities.
- Monitor brand information traffic to mitigate potential vulnerabilities or exploitation points found and generate alerts of possible compromised data to the Risk and Compliance area, reporting any cyber risk that impacts the business without an adequate mitigation plan.
- Ensure the implementation of multi-factor authentication and other practices to ensure control of access to company assets and information.
- Management of Information Technology and Security suppliers.

8.4. Commercial / Marketing

- Observe KYC and KYP processes for Clients and Business Partners.
- Observe the KYP process regarding Suppliers through registration and verification of provided information, as applicable.
- Observe the KYE process regarding Employees in sales actions, campaigns, prospecting, advertising, and provision of gifts, awards, as applicable.

8.5. Financial / Controller

- Maintain MRB's good performance by creating methodologies and systems that develop management controls, working together with the Risk and Compliance area for process optimization and mitigation of AML/CFT risks and indications of crimes.
- Establish procedures for treasury functions, accounts payable and receivable control, third-party resource management, accounting, planning, tax management, and control of potential fraud risks.

8.6. Operations

- Observe KYC, KYS, and KYP processes for Clients, Suppliers, and Business Partners regarding operational, logistical, accreditation, account opening, and Client activation processes.

8.7. Purchasing

- Observe the KYS process regarding Suppliers through registration and verification of provided information after the request for proposals, quotations, or other applicable contracting procedures.

8.8. Human Resources

- Establish criteria and KYE processes for selecting and hiring Employees who have a profile consistent with this Policy, considering the level of responsibility of individuals according to the functions and responsibilities assigned to them.

9. INTERNAL RISK ASSESSMENT (IRA)

- The Internal Risk Assessment defines the methodologies, parameters, techniques, and tools necessary to identify and measure the risk of using MRB's products and services in the practice of ML/TF. To this end, we follow the recommendation of Circular BCB No. 3,978/2020, considering, at a minimum, the following **risk profiles**:
  - *Clients;*
  - *Institution, including the business model and geographical area of operation;*
  - *Operations, transactions, products, and services, covering all distribution channels and the use of new technologies;*
  - *Activities performed by employees, partners, and third-party service providers.*
- The identified risk must be assessed for its probability of occurrence and the magnitude of financial, legal, reputational, and socio-environmental impacts on MRB.
- Four (4) **risk categories** are defined: Very High Risk / High Risk / Medium Risk / Low Risk.
  - These categories allow for the adoption of strengthened management and mitigation controls for situations of higher risk and the adoption of simplified controls for situations of lower risk.
  - The final score represents the same percentages indicated in the risk matrix (probability versus impact table) included in the AIR.
- Assessments conducted by public entities in the country regarding the risk of money laundering and terrorist financing should be used as a subsidy for internal risk assessment when available.
- The internal risk assessment must be:
  - Documented and approved by the Director responsible, before the Central Bank of Brazil, for compliance with MRB's AML/CFT management obligations.
  - Forwarded for awareness to the institution's Board of Directors; and
  - Reviewed every two (2) years, as well as when significant changes occur in the risk profiles used.

10. EFFECTIVENESS ASSESSMENT

- The Effectiveness Evaluation must be capable of verifying compliance with this Policy, related AML/CFT procedures, and internal controls, as well as identifying and correcting identified deficiencies and opportunities for improvement.
- The **Effectiveness Evaluation** must be documented in a **specific report**, which must:
  - Be prepared annually, with a reference date of December 31st; and
  - Be forwarded for awareness to the institution's Board of Directors by March 31st of the following year.
  - Contain information describing:

a) The methodology adopted in the effectiveness evaluation;
b) The tests applied;
c) The qualifications of the evaluators; and
d) The deficiencies identified;

- Include, at a minimum, an evaluation of:
  a) Procedures for client due diligence, including verification and validation of client information and the adequacy of registration data;
  b) Monitoring, selection, analysis, and reporting to the COAF procedures, including effectiveness evaluation of transaction selection parameters and suspicious situation criteria;
  c) Governance of the anti-money laundering and counter-terrorism financing policy;
  d) Measures to develop organizational culture aimed at preventing money laundering and terrorist financing;
  e) Periodic staff training programs;
  f) Procedures for knowing employees, partners, and third-party service providers; and
  g) Actions to address findings from internal audit and Central Bank of Brazil supervision.

- An **Action Plan** should be developed to address deficiencies identified in the Effectiveness Evaluation and outlined in the report.
  - The implementation of the Action Plan should be monitored and documented through a Monitoring Report.
  - The Action Plan and corresponding Monitoring Report should be forwarded for awareness and evaluation by the institution's Board of Directors by June 30th of the year following the report's reference date of the Effectiveness Evaluation.

11. DUE DILIGENCE

- Data provided in KYC, KYS, and KYP procedures will be verified through the submission of documents and/or by querying public or private databases, such as credit and risk analysis bureaus, as well as internal databases or those shared by other companies.
- Processes are checked with courts, negative media, and restrictive lists to investigate possible involvement of the third party/proponent in illicit activities. Third-party monitoring occurs continuously, where judicial processes, CNPJ status with the Federal Revenue Service, among others, are verified.
- Information obtained in KYC, KYS, and KYP procedures will be stored, compatible with the risk profile defined by the Risk and Compliance area, according to the nature of the business and the risk to which MRB will be exposed.
- *Due diligence* will be conducted systematically and periodically.
- Registration information will be archived for a minimum period of 5 (five) years, starting from the first day of the year following the end of the relationship with the Client, Supplier, or Business Partner.
  - After this period, the disposal of information must comply with the General Data Protection Law (Law No. 13709/2018), as applicable, and specific legislation applicable to MRB's business activities.
- Updating of data pertaining to Clients, Suppliers, and Partners must occur systematically and periodically.
  - However, tests should be conducted every 12 months to validate registration and registration information, so that any inconsistencies found should be promptly rectified for regularization.

12. KNOW YOUR CLIENT (KYC)

12.1. Know Your Client (KYC)

- MRB will implement a *Know Your Client (KYC) Policy*, containing specific provisions and regulations aimed at adopting prior and periodic due diligence to ensure identification, qualification, and classification of its Clients, thereby preventing ML/TF occurrences.
    - Procedures are adopted to identify and validate the identity and integrity of the client, including obtaining, verifying, and validating the authenticity of their identification information by cross-referencing this information with lists available in public and/or private databases (as provided in item 11 of this Policy), when necessary, and according to the client's risk category.
    - At any time, including after registration, supplementary information, declarations, and documents may be requested for validation purposes.
    - Procedures are adopted to qualify MRB's clients by collecting, verifying, and validating information compatible with the client's risk profile and the nature of the business relationship to be conducted.
- Only potential clients whose activities are lawful, fully compliant with the law, and with updated, valid, and current documentation before relevant competent authorities will be considered as potential clients of MRB.
- Client registration will be conducted individually and standardized, containing all personal data and information required by applicable legislation.
- Specific classification will be applied to clients considered as PEP.
- For the purpose of *Combating the Financing of Terrorism*, potential Clients included in the OFAC list will not be approved for registration.
- Risk classification will be reviewed whenever there are changes in the client's risk profile and the nature of the business relationship.

12.2. Politically Exposed Persons (PEP)

- MRB will implement procedures to classify its clients as Politically Exposed Persons (PEPs) without exception, defined as individuals holding significant public functions within various branches of government, as per the list provided in Circular BCB No. 3,978/2020.
- Qualification procedures include consulting publicly and privately available lists or through self-declaration included in each client's registration.
- The decision to initiate or maintain a client relationship classified as a PEP is based on risk perception, made by managers of higher hierarchy than the one responsible for approving the registration activity. If the decision is positive, it must be submitted to the Risk and Compliance area, which exclusively holds the authority to approve or decline the continuation.
- If approved, the respective areas must report all transactions conducted by PEP clients to the Risk and Compliance area.

12.3. Ultimate Beneficial Owner

- In the qualification procedures for legal entity clients, the chain of corporate ownership is analyzed until the identification of the natural person characterized as its ultimate beneficial owner, for whom, at a minimum, the qualification procedures defined for the risk category of the legal entity client in which the ultimate beneficial owner holds corporate participation will be applied.

- MRB also considers as ultimate beneficial owner any representative, including attorneys-in-fact and authorized agents, who exercise effective control over the activities of the legal entity client.
- In situations involving clients with special corporate configurations (as listed in paragraph 3 of article 24 of Circular BCB No. 3,978/2020), the chain of corporate ownership is not analyzed. Instead, information is collected covering the natural persons authorized to represent them, as well as their controllers, administrators or managers, and directors, as applicable.

12.4. Operational Limits

- The definition of operational limits is established based on an examination of the client's financial capacity (revenue, considering the current profile of clients being legal entities), while ensuring compatibility and proportionality with the level of risk.
- The documentation required from clients to prove financial capacity will have its type and form defined according to the respective purpose of the business relationship, products or services consumed, as well as the nature of their operations.

13. PARTNERS AND SUPPLIERS SELECTION (KYP E KYS)

- Suppliers or Business Partners will be verified according to their business activity, profile, and purpose of the relationship, including information about the third party with whom the contract will be entered into, any business relationship established, or sponsorship granted.
- The risk classification of the supplying/partnering company will occur according to the internal regulations of the *Risk and Compliance* area, allowing the refusal of contracting with any Supplier or Business Partner based on KYS and KYP procedures.
- If the business or professional activity carried out by the company is classified as high risk, the Operational, Financial, and Risk and Compliance areas will establish enhanced monitoring of the values involved.
- The remuneration to be paid by MRB, regardless of its nature, must be settled in a payment account or bank account owned by the respective Supplier or Business Partner.
- Obligations related to AML/CFT must be necessarily included in the contracts to be entered into with Suppliers and Business Partners.
- *Due diligence* will be conducted as established in item 11 of this Policy.

14. EMPLOYEES SELECTION AND HIRING (KYE)

- The selection and hiring of Employees, including third parties, will be carried out with the aim of reducing the risk of illicit practices of any nature, including AML/CFT, regardless of the position or function, adhering to specific criteria established in Human Resources procedures, considering the guidelines outlined in this Policy and identified risks.
- During the hiring stage, it is the responsibility of the Human Resources department, following recruitment and selection processes, to conduct a profile analysis, identifying whether the potential employee's characteristics are aligned with MRB's values and current institutional policies, as well as assessing any candidate's potential background that may indicate a potential risk of ML/TF.
- The *background check* procedure and other related processes must be validated by the *Risk and Compliance* area, ensuring the legal compliance of the information collected or validated.
- Preventive monitoring includes regular checks, paying attention to mapped risks.
    - There must be equal treatment in this conduct, encompassing all Employees, with monitoring for discriminatory purposes prohibited.

  - Employees must be informed in advance about this monitoring, either by signing the Form provided in Annex I of this Policy or by explicit mention in their employment contract.
- Managers of MRB's departments are responsible for identifying and informing the *Risk and Compliance* area about behaviors contrary to what is established in this Policy, or other policies and procedures adopted by MRB's Human Resources department.

15. OPERATION REGISTRATION PROCEDURE

- MRB will maintain records of all operations conducted, products and services contracted, including withdrawals, deposits, contributions, payments, receipts, fund transfers, and operations in the foreign exchange market.
- In accordance with Circular No. 3,978/2020, records will be kept with the following minimum information for each operation:
  a) client details;
  b) type and nature of the business;
  c) value;
  d) delivery method;
  e) date of execution;
  f) parties involved;
  g) distribution channels used; and
  h) origin and destination of the resources.
- In the case of operations related to payments, receipts, and fund transfers through any instrument, the records will include necessary information for identifying the origin and destination of the resources.
- The records of operations will include at least information allowing identification of the sender's name and CPF or CNPJ registration number, the payer, the recipient, or the beneficiary, as well as identification codes in the payment settlement or fund transfer system of the institutions involved in the operation.
- For Transaction monitoring, the *Risk and Compliance* area must establish, in addition to the above-mentioned records, the Transaction values and monitoring and selection criteria to identify suspicious Transactions.
- MRB will maintain records of all operations conducted by Clients, which will be archived for a minimum period of 5 (five) years, starting from the first day of the year following the completion of the operation, and in the case of information and records of fund transfers, the period will be 10 (ten) years.
- In accordance with Law No. 14,790/2023, MRB must maintain, in the manner and timeframe established by the Ministry of Finance regulation, records of all operations conducted, including bets placed, prizes won, and withdrawals and deposits in transactional accounts.

16. MONITORING, SELECTION, AND ANALYSIS OF SUSPICIOUS OPERATIONS AND SITUATIONS

- The *Risk and Compliance* area shall define and implement monitoring and selection procedures to identify operations and situations that may indicate suspicion of money laundering and terrorism financing.
  - The period for executing monitoring and selection procedures for suspicious operations and situations shall not exceed 45 (forty-five) days from the date of occurrence of the operation or situation.

    - The analysis conducted must be formalized in a **dossier**, regardless of communication to COAF.
- Technological monitoring tools with automatic alerts for atypical activities shall be used for Transaction monitoring.
    - The systems used must contain detailed information on the operations conducted and situations occurring, including information on the identification and qualification of the individuals involved.
- Transactions that show signs of ML/TF, as determined by the monitoring procedures instituted by the *Risk and Compliance* area, may be automatically rejected and canceled, considering factors such as those exemplified below:
    a) Habituality, value, periodicity, form, or Client's historical relationship with previous Transactions;
    b) Intention to generate gain without justified economic benefit;
    c) Unjustified omission or delay in providing information and/or documents by the Client;
    d) Significant fluctuation in the volume and/or frequency of Transactions;
    e) Sudden and unjustified change in the Transaction's modality or value;
    f) Incompatibility with the Client's financial capacity, considering their previously demonstrated financial capacity;
    g) Continuous repetition of Transactions between the Client and the same beneficiary;
    h) Offsetting of credits and debits between the Client and the same beneficiary;
    i) Client acting on behalf of third parties;
    j) Difficulty or impossibility of identifying the ultimate beneficiary;
    k) Identification of erroneous, untrue, or outdated information from the Client; and
    l) Reports received through the Whistleblower Channel.
- Other situations not covered in the above list may be assessed by the *Risk and Compliance* area.
- MRB shall establish procedures regarding hypotheses and treatments associated with cases of *Enhanced Monitoring* of specific Clients or Transactions due to the high associated risk.
- All processes and procedures related to compliance with item 16 of this AML/CFT Policy shall be defined based on the IAR and the terms of Circular BCB No. 3,978, 2020.

17. REPORTING PROCEDURE TO COAF

- MRB shall report to COAF operations or situations suspected of money laundering and terrorism financing.
- The decision to report the operation or situation to COAF must:
    a) Be based on the information contained in the operation analysis dossier.
    b) Be detailedly recorded in said dossier.
    c) Occur by the end of the analysis period - 45 (forty-five) days from the date of selection of the suspected operation or situation.
- The report must specify, when applicable, whether the individual subject of the report:
    a) Is a PEP or a representative, family member, or close associate of such person.
    b) Is a person who has been recognized as having committed or attempted to commit terrorist acts or participated in them, in which case it must also be reported whether the person owns or controls, directly or indirectly, resources in the institution.
- The report of the suspected operation or situation to COAF must be made by the next business day following the decision to report.

- The report must be made without informing the parties involved or third parties.
- Reports altered or canceled after the fifth business day following their issuance must be accompanied by a justification for the occurrence.

18. COMMUNICATION AND TRAINING

- This Policy is applied and widely disseminated by Senior Management, through the *Risk and Compliance* department, to all employees of MRB, as well as its branches, subsidiaries, and representative offices, if any, and service providers, as applicable, in clear and accessible language, considering the functions performed and the proper sensitivity of the information provided.
- Various communication channels may be used, including: *the MRB website, corporate communication email, and a link to access the Policy inserted in contracts signed with service providers and third parties.*
- For the purpose of maintaining awareness levels continuously, MRB must conduct prevention actions through awareness campaigns on the topic and periodic corporate training (which may include an internal evaluation process for participants, when necessary), as well as through the periodic updating of internal regulations related to it.
- Internal regulations and procedures related to AML/CFT must be periodically reviewed.
- Questions and suggestions can be addressed through the contact *compliance@mrbdigitais.com.br*

19. VIOLATION AND SANCTIONS

- Any breaches or suspicions of violations of the provisions of this Policy must be immediately reported to MRB's Whistleblower Channel, which will handle the occurrences appropriately via email *ouvidoria@mrbdigitais.com.br*, through receipt, preliminary analysis, classification, treatment, monitoring, investigation, decision-making, reporting of complaints, and closure of occurrences.
  - MRB will receive and act on reports from Administrators, Employees, Suppliers, Clients, Business Partners, or any third parties regarding atypical or suspicious activities that may constitute indications of crimes related to Money Laundering and Terrorism Financing.
  - Reports will be received by a qualified and empowered professional, ensuring anonymity and confidentiality of communications, as well as preserving the integrity of the whistleblower.
- Non-compliance with the applicable AML/CFT legislation, besides potentially causing serious damages to MRB, may subject the offender to criminal, civil, and administrative penalties by the authorities.
  - Additionally, the infringing employee may face disciplinary measures based on applicable legislation, including verbal or formal warnings, suspension, monetary sanctions, and potentially termination for just cause, without prejudice to the adoption of legal measures.
  - Other penalties stipulated in legally valid contracts may also be imposed.

20. FINAL PROVISIONS

- Any omissions or exceptions to the provisions of this Policy or those requiring specific approval must be submitted for formal evaluation by the Directorate responsible for *Risk and Compliance* management at MRB.
- This Policy is accompanied by an *Acknowledgment Form for AML/CFT* and an *Acknowledgment Form for Amendments to this AML/CFT Policy*.
  - All MRB employees must read, understand, and formally acknowledge their awareness and commitment to this Policy by signing the available forms.

- The personal data provided when filling out the form(s) will be duly stored by MRB in accordance with applicable legislation.
- All contracts entered into with service providers, partners, and third parties throughout the contractual term must contain a clause acknowledging and committing to compliance with this Policy, shared as provided in item 10.

21. EFFECTIVENESS, REVIEW, AND AMENDMENTS

- This Policy shall enter into force upon its publication, repealing any conflicting provisions, and shall remain in effect indefinitely.
- It will be reviewed and updated **annually** (or more frequently if necessary for effectiveness, risk adequacy, best practices, or legal/regulatory compliance) by the *Risk and Compliance* area, and submitted for approval by the Senior Management, in accordance with their internal responsibilities, followed by subsequent publication.

Date	Version	Description	Authors
March 11, 2024	1.0	Elaboration	External Consulting
April 02, 2024	1.0	Approval	Raquel Birck – Managing Partner

22. ANNEXES

ANNEX I – AML/CFT ADHERENCE FORM
ANNEX II – AML/CFT AMENDMENT ADHERENCE FORM

ANNEX I – AML/CFT ADHERENCE FORM

I, _____ , enrolled in the CPF under no. _____, declare that I am aware of this *Anti-Money Laundering and Combating the Financing of Terrorism Policy (AML/CFT)*, as well as the guidelines contained in other related policies, norms, and internal procedures of MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA.

I am aware of the activities of MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA and of how it may be exploited for the commission of money laundering and terrorism financing crimes. Therefore, within the duties of my role, I must, whenever necessary, utilize the Whistleblower Channel to report any type of suspicious activity and/or activity deemed criminal by this Policy and by MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA.

Location: _____ Date: _____

Full Name: _____

Signature: _____

ANNEX II – AML/CFT AMENDMENT ADHERENCE FORM

I, _____ , enrolled in the CPF under no. _____, declare that I am aware of the changes made in this *Anti-Money Laundering and Combating the Financing of Terrorism Policy (AML/CFT)*, as well as the guidelines contained in other related policies, norms, and internal procedures of MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA.

I am aware of the activities of MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA and of how it may be exploited for the commission of money laundering and terrorism financing crimes. Therefore, within the duties of my role, I must, whenever necessary, utilize the Whistleblower Channel to report any type of suspicious activity and/or activity deemed criminal by this Policy and by MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA.

Location: _____ Date: _____

Full Name: _____

Signature: _____