MRB INTERMEDIAÇÃO E NEGÓCIOS DIGITAIS	Know Your Client (KYC) Policy	Code:	POL-RC-003
		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.
- **API** – *Application Programming Interface* – a set of rules and protocols that facilitates communication between different software applications, enabling them to interact with each other in a standardized and secure manner.
- **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 Real and foreign currency. It consists of two segments: Financial Market Infrastructures (IMF) and Payment Arrangements.
- **Client** – Legal entity duly qualified to purchase products or services offered by MRB.
- **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.
- **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.
- **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.
- **LGPD** – "Lei Geral de Proteção de Dados Pessoais" – General Data Protection Law (Law No. 13,709/2018).
- **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.
- **Opportunities for improvement** – Areas or processes that can be enhanced to increase efficiency, quality, or results.
- **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.

- **Proponent** – Legal entity showing interest in becoming a client of MRB, either through a formal business proposal or through informal expression of interest.
- **Risk 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 directing the overall course of the organization.

2. INTRODUCTION

The *Know Your Client* (KYC) Policy establishes a set of stringent procedures and controls adopted by payment institutions to acquaint themselves with their respective Clients, through the adoption of prior and periodic diligence ensuring their identification, qualification, and classification, thus preventing Money Laundering and Terrorism Financing. This enables an understanding of the nature of their activities and assessment of associated risks.

These practices necessitate the maintenance of accurate and updated records, conducting periodic due diligence, and proactive communication with regulatory authorities upon the discovery of suspicious activities.

Thus, this Policy not only bolsters financial security but also fosters transparency and trust between the institution and its clients.

3. OBJECTIVE

Through this Policy, MRB aims to:

- Adopt procedures allowing for the identification and validation of the client's identity and integrity, including obtaining, verifying, and validating the authenticity of their identification information by comparing it with available lists in public and/or private databases, when necessary, and in accordance with the client's risk category.
- Establish specific provisions and regulations aimed at adopting prior and periodic diligence to ensure their identification, qualification, and classification for client knowledge, thus preventing occurrences of ML/TF.

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

- **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. 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.
- **Law No. 13,709, dated August 14, 2018** (and amendments) – "Lei Geral de Proteção de Dados Pessoais" – General Data Protection Law (LGPD).
- **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.
- **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).
- **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.
- MRB's **Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Policy.**
- MRB's **Risk Management Policy**.

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

In the event that MRB applies for authorization to operate as a Payment Institution to the Central Bank, pursuant to Law No. 12,865 of October 9, 2013, and Central Bank Resolution No. 80/2021, MRB will undertake the necessary measures to comply with Joint Resolution No. 6 of May 23, 2023, and Central Bank Resolution No. 343 of October 4, 2023, pertaining to the sharing of data and information regarding indications of fraud.

6. GENERAL PROVISIONS

- KYC procedures must be formalized in specific manuals and be compatible with:
  a) The client's risk profile, encompassing enhanced measures for clients classified in higher-risk categories;
  b) The AML/CFT Policy[1];
  c) Internal Risk Assessment (IRA)[2]
- KYC procedures must adhere to LGPD, adopting robust security measures to protect sensitive information collected from applicants/clients against unauthorized access or privacy breaches.

[1] Special attention should be given to the *"Due Diligence"* and *"Reporting Procedure to COAF"*, when applicable, as well as the guidelines outlined in the *"Know Your Client (KYC)"* and its subsections.
[2] Refer to Item 13 of the *Risk Management Policy* and Item 9 of the *AML/CFT Policy*.

- Information obtained and utilized in KYC procedures must be stored in computerized systems and used in monitoring, selection, and analysis of suspicious operations and situations. To this end, parameters and best practices of Information Security established by the responsible area must be complied with.
- This policy should be understood in conjunction with other pertinent institutional policies, and its content does not substitute nor prevail over any legal instrument.

7. ROLES AND RESPONSIBILITIES

KYC procedures demand a rigorous verification of clients' identity and history, and it's essential that each function within the financial institution clearly understands its responsibilities in this process.

Without a clear definition of roles and responsibilities, MRB risks failing in its processes, which may result in regulatory violations, significant fines, and damage to the company's reputation. Therefore, it's crucial that each department and member understand their specific role in complying with this Policy.

7.1. Senior Management

- Ensure institutional adherence to best practices of registration, KYC, and AML/CFT compliance with current laws and regulations.
- Approve the drafting, review, and amendments to this Policy for subsequent publication.

7.2. Risks and Compliance

- Verify the adequacy of client registration data, guiding the responsible management for Registration on the need for corrections and opportunities for improvement in registration processes to prevent the use of the institution's structure for ML/TF.
- Report to the Registration department the need for corrections and implementation of best registration practices.
- Support the Registration department for best practices in handling information and documentation from applicants and clients.
- Manage tools and establish processes related to background checks and due diligence.
- Ensure compliance of business areas and all internal MRB procedures.
- Coordinate communication and training for Administrators and Employees.
- Ensure compliance with the Whistleblower Channel mechanisms.
- Monitor occurrences of suspicious or atypical transactions identified by MRB's technological tools or reported by Employees.
- PEP classification and monitoring, when necessary.
- Communication with COAF and Central Bank, as well as compliance with audits and other regulatory bodies and competent authorities.
- Promote effective communication of the Policy through institutional channels and training.
- Verify any updates, revocations, and the issuance of new regulations.
- Conduct periodic review of the Policy.
- Analyze omissions or exceptions to the provisions of this Policy (via Management, as per Item 13).

7.3. Commercial / Marketing

- Support the Registration and *Risks and Compliance* departments with appropriate and necessary information and documents regarding prospective clients and their operations.
- Follow MRB's established procedures for KYC.
- Contact the *Risks and Compliance* department in case of procedural doubts, uncertainties regarding clients and documents, as well as suspicions and cases to be reported that they become aware of.

7.4. Registration

- Collect, register, analyze, and validate information and identification documents of clients with whom MRB maintains a relationship.
- Report difficulties, vulnerabilities, and improvement opportunities to IT/IS related to MRB's registration systems.
- Establish periodic review of registered clients.
- Manage the registration of active, inactive, suspended, and other status classifications standardized by MRB.

7.5. Finance / Controllership

- Implement AML/CFT controls related to client behavior to internally report suspicious operations.
- Implement necessary processes in case of blocking, restrictions, as well as other necessary situations according to legal provisions and guidance from the *Risks and Compliance* department.

7.6. Information Technology / Information Security

- Ensure that computerized systems used in monitoring, selecting, and analyzing suspicious operations and situations are available and provide reliable and integral information.
- Promote improvements in the infrastructure supporting client registrations.
- Establish parameters and best practices of Information Security for MRB's products, services, and operations.
- Ensure full compliance with access restrictions to systems, approvals of electronic processes, changes in system rule parameters, and others, formalized, implementing Role-Based Access Control, Information Security Policy, and other necessary internal norms and procedures.
- Test cybersecurity controls for fraud prevention.
- Act diligently in protecting and maintaining the confidentiality of data and technological tools and infrastructure of MRB.
- Monitor and manage the security of all applications, systems, communication with suppliers, and MRB's technology structures to mitigate any risk of manipulation, cyber attacks, or exploitation of systemic vulnerabilities.
- Ensure the implementation of multi-factor authentication and other practices to ensure control of access to company assets and information.
- Manage Information Technology and Security suppliers.

8. CLIENT CLASSIFICATION

These are the types of clients of MRB:

8.1. Direct Clients

- Brazilian legal entities, duly incorporated and registered under an active and valid CNPJ with the Brazilian Federal Revenue Service, with lawful corporate purpose and activities, having an ongoing relationship with MRB for the provision of payment services in accordance with terms, policies, and legal provisions.

8.2. Users (transient)

- Individuals who are not clients of MRB but of the companies that have contracted MRB to process payments. The registration of these users is done with minimal and automated information, with merely operational and control-related relationship.
- *Due diligence* of the user is carried out by the client company within its environment.
- The user is subject to MRB's internal AML/CFT controls and established operational limits.

- MRB will establish a communication mechanism with client companies to report suspicious or anomalous activities of these users, or to inform about any applied blocks and suspensions.

9. KNOW YOUR CLIENT (KYC) PROCEDURES

MRB primarily employs electronic KYC approaches through the use of systems to ensure impersonality and record of inquiries. These procedures are:

i. Registration;
ii. *Due diligence*;
iii. Definition and monitoring of operational limits.

9.1. Registration

- In MRB's ***Registration Policy***, the following can be consulted:
  - Guidelines and detailed rules for client registration;
  - Client status (qualification).
- Depending on the purpose of opening the account, the Commercial and Registration departments should provide client information for filling out the *Registration Form* in the system. Therefore, the following client information will be minimally collected:
  a) CNPJ Card;
  b) Articles of Association;
  c) Personal documents of Shareholders (ID, CPF, updated proof of address);
  d) Identification of the Managing Partner;
  e) Revenue (financial information such as Balance Sheet, Income Statement, Revenue Projection);
  f) Email for registration;
  g) Mobile phone number for registration;
  h) Focal points (key persons for contact in operations).
- If the Client conducts business or professional activities in a physical establishment, MRB or a Commercial Partner (if applicable) may, physically or remotely (including using geolocation technologies), verify the effective existence of the establishment at the indicated location.

9.2. Data Queries and *Due Diligence*

9.2.1. Data and Information Collection

For *due diligence* and information cross-referencing purposes, clients (and their legal representatives) will have their data and information queried in public and private databases and lists of sanctions and restrictions, checking, for example:

- Politically Exposed Person (PEP) validation rule (Verifies if a person is considered a PEP);
- Individuals on the OFAC SDN[3] list;
- Name on the Federal Revenue Service (regularity of CPF);
- Death registry at the Federal Revenue Service (no death record should appear in the Federal Revenue Service);
- Date of Birth at the Federal Revenue Service (Date of Birth must match the one registered with the Federal Revenue Service);
- Regular Tax Situation (CPF registration status must be REGULAR);
- Criminal Background (no criminal records should appear);

[3] *Specially Designated Nationals and Blocked Persons List* ("SDN List") is the roster of individuals specially designated and blocked persons, commonly known as the OFAC list.

- Warrants with Homonyms (checks for the existence of warrants for the searched name, using mother's name and date of birth to aid in disambiguating homonyms);
- Company registration consultation at the Federal Revenue Service (company name, corporate purpose, corporate structure, legal entity status (active, inactive, dissolved, suspended, etc.), business address, registration update, contact information);
- Analysis of the Articles of Association or Bylaws;
- Court cases and derogatory media are verified.

9.2.2. Auxiliary Verification Tools

The following may be used as aids in MRB's *due diligence* process:

- Identity validation systems;
- Data query software;
- Photo captured with the submitted document's photo.

9.2.3. Information Updates, Timelines, and Data Retentions

Considering that KYC procedures reflect a historical and current economic/financial situation and condition, it becomes necessary to maintain updates and supplementation of the information initially provided by Clients.

- Client information will be periodically updated, not exceeding a period of 12 (twelve) months, or whenever any of the departments involved in the process (Commercial, Registration, Compliance, Management) deem it necessary.
- The outcome of KYC and due diligence checks may alter the client's qualification, potentially rendering them temporarily or permanently unfeasible.
- Refer to item 11 of the *AML/CFT Policy* for further data retention periods and requirements.

9.3. Operational Limits

- MRB establishes risk mitigation criteria in client accreditation, considering the risk profile, by setting a maximum limit for transactions within specified periods.
- Operational limits and the mechanism for monitoring client behavior are described in the ***Policy for Monitoring and Analyzing Operations and Suspicious Situations***, in accordance with MRB's *Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Policy*.
    - The definition of operational limits is based on an examination of the client's financial capacity (revenue, considering the current profile of clients being legal entities), with due regard to the compatibility and proportionality of the risk level.
    - 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.
    - The alteration of limits, where possible, will consider, among other factors, the financial capacity of the client company, necessitating the presentation of complementary documents.

10. CLIENT BLOCKING AND REFUSAL

Regarding the evaluation of the client, MRB does not engage with its own clients, users (transient), or proposers (initial business relationship) falling under the following circumstances and must be summarily rejected:

10.1. Direct Clients

- Suspicious circumstances and/or evidence related to practices of corruption, money laundering, terrorist financing, fraud, concealment of information, socio-environmental responsibility crimes, practices of slave labor, as well as other illicit activities or violations of rights;
- If occurrences are found in sanctions and restrictions lists during investigations.
- If the client goes against MRB's values or violates its institutional policies.

10.2. Users (transient)

- Suspicious circumstances and/or evidence of irregularities regarding transient clients, with direct blocking done in the API.
- MRB's *due diligence* tools and processes may be used to support decision-making.

Client blocking and refusals may occur according to situations established in the *Policy for Monitoring and Analyzing Operations and Suspicious Situations*.

11. COMMUNICATION AND TRAINING

- This Policy is applied and widely disseminated by Senior Management, through the *Risk and Compliance* department, to MRB employees involved in: client acquisition, commercial activities, registration, customer service and ombudsman, compliance; as well as operational, financial, and internal control activities.
- Various communication channels may be utilized, including: *MRB's website, corporate communication emails, and a link for accessing the Policy*.
- Periodic corporate training sessions may be conducted (with the possibility of implementing an internal participant evaluation process, when necessary).
- Internal regulations and procedures related to KYC shall be periodically reviewed.
- Questions regarding this Policy may be addressed via email: *compliance@mrbdigitais.com.br*

12. VIOLATIONS AND SANCTIONS

- Any breaches or suspicions of violations of the provisions of this Policy should be immediately reported to MRB's Whistleblower Channel, which will appropriately handle the incidents via email at *ouvidoria@mrbdigitais.com.br*. This includes receipt, preliminary analysis, classification, treatment, monitoring, investigation, decision-making, reporting of complaints, and closure of incidents.
    - MRB will receive and act upon reports from Administrators, Employees, Suppliers, Clients, Business Partners, or any third parties, concerning atypical or suspicious activities that may constitute evidence of crimes related to Money Laundering and Terrorist Financing.
    - Reports will be received by a trained professional with the necessary autonomy, ensuring anonymity and confidentiality of communications, as well as the preservation of the whistleblower's integrity.
- Non-compliance with applicable laws, besides potentially causing severe harm to MRB, may subject the offender to criminal, civil, and administrative penalties by the authorities.
    - Moreover, the offending employee will be subject to disciplinary measures under applicable law, including verbal or formal warnings, suspension, and monetary sanctions, which may ultimately lead to dismissal with cause, without prejudice to the adoption of legal measures.
    - Additional penalties stipulated in legally valid contracts may also be imposed.

13. FINAL PROVISIONS

- Any omissions or exceptions to the provisions established in this Policy, or matters requiring specific approval, shall be submitted for formal evaluation by the Management Board responsible for *Risk and Compliance* at MRB.
- The KYC process will inform the development of the *Registration Policy* and the *Policy for Monitoring and Analyzing Operations and Suspicious Situations*.

14. EFFECTIVENESS, REVIEW, AND AMENDMENTS

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

Date	Version	Description	Authors
March 25, 2024	1.0	Elaboration	External Consulting
April 02, 2024	1.0	Approval	Raquel Birck – Managing Partner