MRB INTERMEDIAÇÃO E NEGÓCIOS DIGITAIS	Registration Policy	Code:	POL-RC-004
		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 enables communication between different software, allowing applications and systems to interact with each other in a standardized and secure manner.
- **Applicant** – A legal entity expressing interest in becoming a client of MRB, either through a formal business proposal or an informal expression of interest.
- **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** – A legally qualified entity to acquire 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.
- **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.

- **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.
- **Ultimate Beneficiary** – Individuals who ultimately own, control, or influence an organization, even indirectly.

2. INTRODUCTION

The *Registration Policy* is a vital extension of the *KYC (Know Your Client) Policy*, providing specific guidelines for the identification, validation, and continuous monitoring of clients, playing a fundamental role in preventing money laundering and combating terrorist financing.

While the *KYC Policy* establishes the general principles for identifying and validating clients, the Registration Policy offers more specific and operational guidelines for implementing these principles in the institution's day-to-day practice, thereby becoming an essential tool for MRB in mitigating risks related to its clients.

3. OBJECTIVE

Through this Policy, MRB aims to:

- Ensure, through rigorous processes of collecting and verifying personal information, that clients are not involved in illegal activities such as money laundering or terrorist financing.
- Ensure the integrity of the registration process and maintain regulatory compliance.

4. SCOPE

This Policy applies to all individuals within MRB, focusing directly on the handling of Clients, but also encompassing managers, investors, employees, interns, service providers, consultants, and other individuals or legal entities that use or support the business of the Payment Institution.

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 Combating the Financing of Terrorism (AML/CFT) Policy**.
- MRB's **Risk Management Policy**.
- MRB's **Know Your Client (KYC) 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

- MRB is prohibited, under the law[1], from initiating a business relationship without the completion of client *Identification* and *Qualification* procedures.
    - Initiation of a business relationship may be permitted for a maximum period of 30 (thirty) days in case of insufficient information regarding client qualification, provided that there is no detriment to the monitoring and selection procedures that enable the identification of operations and situations that may indicate suspicions of ML/TF.
- Registration procedures must be formalized in *specific manuals*, which should outline the criteria used to define necessary information and verification, validation, and updating procedures for each risk category.
    - Procedures must comply with LGPD, adopting robust security measures to protect sensitive information collected from applicants/clients against unauthorized access or privacy breaches.
- Information obtained and used in the registration process must be stored in computerized systems, according to Information Security parameters and best practices established by the responsible department. This information will be used in the selection and monitoring procedures of these clients.
- The identification, qualification, and classification procedures outlined in this Policy must be adopted by MRB for corporate client administrators and client representatives.

[1] Article 23, *caput*, of Circular No. 3,978 dated January 23, 2020.

  - Such procedures must be compatible with the function performed by the administrator and the scope of representation.
- This policy should be understood in conjunction with other relevant institutional policies, and its content does not replace or take precedence over any legal instrument.

7. ROLES AND RESPONSABILITIES

Clearly outlining the roles and responsibilities in client onboarding at MRB ensures that each team member understands their specific functions within the Know Your Client (KYC) process, from the initial collection of information to the verification and continuous updating of data. This helps to avoid gaps or overlaps in the client onboarding process, enabling potential shortcomings to be identified and remedied more effectively.

7.1. Senior Management

- Ensure institutional adherence to best practices in client onboarding, KYC, and AML/CFT, complying with relevant laws and regulations.
- Approve the drafting, revision, and changes to this Policy for subsequent publication.

7.2. Risk and Compliance

- Verify the adequacy of institutional client registration data, guiding the management responsible for Registration on correction needs and opportunities for improvement in onboarding processes to prevent the misuse of the institution's structure for ML/TF crimes.
- Conduct verification of the adequacy of institutional client registration data.
- Report to the Registration department on the need for corrections and implementation of best registration practices.
- Support the Registration department 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 procedures of MRB.
- Create and coordinate communication and training for Administrators and Staff.
- Ensure compliance with the mechanisms of the Whistleblower Channel.
- Monitor occurrences of unusual or suspicious transactions identified by MRB's technological tools or reported by Staff.
- Classification and monitoring of PEPs, when necessary.
- Communication with COAF and Bacen, as well as handling audits and other supervisory bodies and competent authorities.
- Promote effective communication of the Policy through institutional channels and training.
- Check for 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 the Board, as per item 18).

7.3. Commercial / Marketing

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

7.4. Registration

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

7.5. Financial / Operations

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

7.6. Information Technology / Information Security

- Ensure that computerized systems used in monitoring, selection, and analysis of suspicious operations and situations are available and provide reliable and comprehensive information.
- Promote improvements in the infrastructure supporting client registrations.
- Establish Information Security parameters and best practices 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 other formalized determinations, implementing Role-Based Access Management, Information Security Policy, and other necessary internal regulations and procedures.
- Test cybersecurity controls to prevent fraud.
- Act diligently to protect and maintain the confidentiality of data and MRB's technological tools and infrastructure.
- 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.
- Management of IT and Security vendors.

8. CLIENT IDENTIFICATION

- Data collected through the Registration Form is described in item 9.1 of the *KYC Policy*.
- Parameters for *Due Diligence*, for verifying and validating the authenticity of client identification information, are outlined in item 9.2 of the *KYC Policy*.
    - Item 9.2.1 of the *KYC Policy* lists the main sources of restricted lists and public/private inquiries.
- Client Administrators must be properly identified, presenting minimum documents:
    - ID card (or other legally accepted identification document).
    - CPF (Brazilian taxpayer registry).
    - Proof of current address (issued within the last 90 days and in their own name).
- If the legal representative of the client (who will sign on their behalf) is a different person from the managing partner (e.g., CEO), they must present a document legitimizing their representation (e.g., power of attorney, board meeting minutes, etc.).
- Minimum registration information shall adhere to the guidelines provided by the regulations governing this policy, with the possibility of expansion or reduction in accordance with operational

requirements or the characteristics of the products and services, based on the exigency of information and/or documents.

9. CLIENT QUALIFICATION

9.1. Qualification process

- The process aims to qualify clients through the collection, verification, and validation of information, consistent with the client's risk profile and the nature of the business relationship.
- Information collected in the qualification process includes:
  a) Document containing the identification of the headquarters or branch location, considering the client as a legal entity.
  b) Document allowing the assessment of the client's financial capacity (the legal entity's revenue) [2].
- Additional client information compatible with the risk of using products and services in ML/TF practices must be collected.
- Client qualification must be continuously reassessed in line with the evolution of the business relationship and risk profile.
- Information collected during client qualification must be kept up-to-date.
- Verification of the client's status as a Politically Exposed Person (PEP) should be conducted, or for confirmation of their classification, open sources and public and private databases should be consulted.

9.2. Ultimate Beneficiary

- The client qualification procedures for legal entities must include the analysis of the corporate ownership chain until the identification of the natural person characterized as its ultimate beneficiary.
- AML/CFT guidelines for KYC, including the concept of *Ultimate Beneficiary*, can be found in item 12.2 of the *AML/CFT Policy*.
- MRB must establish a minimum threshold of corporate ownership for the identification of ultimate beneficiaries, based on risk and not exceeding 25% (twenty-five percent), considering both direct and indirect ownership.
- The minimum reference value of equity participation must be justified and documented in the procedural manual referenced in item 6 of this Policy.

9.3. Qualification status

The qualification process assigns a nomenclature to the client, according to their status with MRB:

9.3.1. Registered Clients

- Clients who have filled out their registration forms on the registration platform but have not attached documents for the company's analysis.
- They have only passed through a screening process by the Commercial department during client acquisition, but the submission of necessary information and documents for *due diligence* is still pending.

9.3.2. Pending Clients

- Two types of situations:

[2] Provisions regarding Operational Limits are outlined in item 9.3 of the *KYC Policy* and in item 12.4 of the *AML/CFT Policy*.

a) Clients whose email confirmation of registration and/or authentication factor is pending; and/or
b) Documentation provided is incomplete, following compliance analysis.

- Until the client rectifies the outstanding issue(s), due to the absence of documents and/or registration information, indications of inconsistency with the AML/CFT Policy, etc., and thus not meeting the minimum requirements, these clients will not be activated, with only the information collected during the preliminary registration.
- Once the outstanding issues are resolved, the client will automatically be classified as "under review," so that the submitted documentation (or information) can be analyzed in the *due diligence* process.

9.3.3. Clients Under Review

- Clients awaiting validation of documents and verification of *due diligence* for the information and documents submitted, with subsequent approval or rejection following the parameters established by the *Risk and Compliance* department.
- If the client has fulfilled the requirements, they will be reclassified as "Active Clients" and allowed to proceed with MRB's service provision steps.

9.3.4. Active Clients

- Clients whose registrations have been formally approved and are eligible to enjoy MRB's services.
- Also, clients with updated documentation and who have been validated in periodic compliance and AML/CFT tests, with no findings warranting a change in client status.

9.3.5. Inactive Clients

- Clients who wish to terminate their transactions and services contracted with MRB and request account closure (inactivation); or
- Clients with no usage of their accounts for a period of 12 (twelve) months, counting from the date of the last transaction.

9.3.6. Blocked Clients

- Clients blocked due to non-submission of requested supplementary documentation by MRB, considering internal control criteria, AML/CFT, and/or regulatory requirements for reporting to Bacen and other supervisory/control authorities.
- The client will be unable to use MRB's services until their situation is regularized.

9.3.7. Rejected Clients

- Clients whose registration requests have been denied according to *due diligence* tools (public databases), MRB's institutional policies (KYC Policy, AML/CFT Policy, Risk Management Policy, among others), and applicable laws.

9.3.8. Politically Exposed Person (PEP)[3]

- PEPs include:
  - Elected officials of the Executive and Legislative branches of the Union;
  - Holders of positions in the Union's Executive branch, including:
    a) Ministers of State or equivalent;
    b) Special Nature or equivalent;

[3] Resolution No. 40, dated November 22, 2021, issued by the Financial Activities Control Council (COAF).

c) President, vice-president, director, or equivalent, of entities of the indirect public administration;
d) Group High Management and Advisory (DAS), level 6, or equivalent;

- Members of the National Council of Justice, the Federal Supreme Court, Higher Courts, Federal Regional Courts, Labor Regional Courts, Electoral Regional Courts, Superior Labor Justice, and Superior Federal Courts;
- Members of the National Council of the Public Ministry, the Attorney General of the Republic, the Deputy Attorney General of the Republic, the Attorney General of Labor, the Attorney General of Military Justice, Deputy Attorneys General of the Republic, and Attorneys General of the States and the Federal District;
- Members of the Court of Auditors of the Union, the Attorney General and Deputy Attorneys General of the Public Ministry with the Court of Auditors of the Union;
- National presidents and treasurers, or equivalent, of political parties;
- Governors and State and Federal District Secretaries, State and Federal District Deputies, presidents, or equivalents, of entities of the state and district indirect public administration, and presidents of Courts of Justice, Military Courts, Courts of Auditors, or equivalents, of the States and the Federal District;
- Mayors, City Councilors, Municipal Secretaries, presidents, or equivalents, of entities of the municipal indirect public administration, and Presidents of Courts of Auditors or equivalents of the Municipalities.

- Also considered politically exposed are individuals who, abroad, hold the following positions:
  - Heads of state or government;
  - Senior-level politicians;
  - Occupants of senior government positions;
  - General officers and senior members of the Judiciary;
  - Senior executives of public companies;
  - Leaders of political parties.
- Leaders of international public or private entities at senior levels are also considered PEPs.
- The PEP status shall be applied for the following 5 (five) years from the date the individual no longer falls within the categories.
- Family members include relatives up to the second degree in the direct line, spouse, partner, stepchild, and stepdaughter.
- The decision to initiate or maintain a relationship with a client classified as a PEP is based on risk perception, conducted by managers at a higher hierarchical level than the one responsible for the account approval activity. If the decision is positive, it must be submitted to the Risk and Compliance department, which exclusively holds the authority to approve or decline further proceedings[4].
  - Upon approval, the respective departments must report all transactions carried out by PEP clients to the Risk and Compliance department.

10. CLIENT CLASSIFICATION

- MRB must classify its clients into risk categories defined in the Internal Risk Assessment mentioned in the *Internal Risk Assessment (IRA)*, based on the information obtained in the Client *Qualification* procedures (collection, verification, and validation of information, consistent with the client's risk profile and the nature of the business relationship).
- The classification must:
  - Be based on the client's risk profile and the nature of the business relationship; and
  - Be reviewed whenever there are changes in the client's risk profile and the nature of the business relationship.

[4]As stipulated in item 12.2 of the AML/CFT Policy.

- In section 8 of the *KYC Policy*, the types of MRB clients were defined:
  - *Direct Clients;*
  - *Users (transients)*.

11. CLIENT RISK ASSESSMENT

This Policy will utilize procedures for identification, validation, and means for identifying applicants, creating veto parameters and measuring the risks involved in initiating the relationship. Additionally, KYC parameters will be used for periodic review of client registration.

5.1 Criteria for Classification of Client Risks

The client acceptance process shall consider, in its risk and KYC analyses, among others, the following criteria:

a) Geographic Location: place of incorporation or nationality, residence in countries considered high risk, as well as border regions. Clients with nationality or capital from countries on restrictive lists (e.g., OFAC) shall not be allowed to maintain a relationship with MRB.

b) Type of Activity: activities conducted by the client that constitute high risk.

c) Products and Services Contracted: the contracted service may have characteristics that, when associated with the client's activity, increase its risk.

d) Identification of PEPs (Politically Exposed Persons): Best efforts shall be made to identify PEPs, considering the relevance of the client's risk with this identification.

e) Identification of Ultimate Beneficial Owners: in order to identify possible connections to illicit activities, including ML/TF. It is necessary to identify the ultimate beneficial owners of all clients. The inability to identify the ultimate beneficial owners shall prevent the initiation of the relationship, except in exceptional cases where it is legally impossible to identify them.

f) Difficulty in Obtaining Documents and Information about the applicant in opening and renewing registrations: The difficulty in obtaining documents and information and their validation significantly increases the risk of clients.

12. UPDATING OF INFORMATION REGISTRATION PROCESS

- MRB will conduct validation tests on information to assess the need for requesting updated documents from clients.
- These validation tests will occur ***annually***, aiming to update the registration of clients who have made any changes to their registration data and to verify the ongoing accuracy of the data maintained in our registration database.
- The tests will include database analyses, information revalidations, document checklists, and other methodologies necessary to comply with this practice.

13. PROCESS OF "BLOCKING" OR "REJECTION" OF CLIENTS

- MRB will conduct validation tests on information to assess the need for requesting updated documents from clients.
- The change of a client's account status to "blocked" or "rejected" will occur immediately upon the identification of the client's compatibility with their respective classification.
- Service and/or operation proposals that are declined due to issues related to AML/CFT will be documented and archived for consultation by supervisory and regulatory bodies, regardless of whether they are reported to the Financial Activities Control Board (COAF).
- Cases of immediate Blocking or Rejection of clients are specified in section 10 of the *KYC Policy*.

14. CLOSURE DUE TO REGISTRATION ISSUES

MRB will exercise its right to terminate the offering of products and services to clients who, if necessary, do not provide the required documents for their registration and updates. The termination process will be conducted in accordance with applicable laws and regulations, while maintaining records/evidence of the procedures carried out for such purposes.

15. ARCHIVING, CONTROL, AND CONSERVATION

The registrations and transaction records must be retained for a minimum period of 5 (five) years, starting from the closure of the account or the conclusion of the last transaction carried out on behalf of the respective client, with the possibility of extending this period.

16. 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 complaints handling, 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 evaluation process for participants, when necessary).
- Internal regulations and procedures related to Registration shall be periodically reviewed.
- Questions regarding this Policy can be addressed via email: *compliance@mrbdigitais.com.br*

17. 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.

18. FINAL PROVISIONS

The omitted cases or exceptions to what is established in this Policy or those requiring specific approval should be submitted for formal evaluation by the Board responsible for *Risk and Compliance* management at MRB.

19. 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 31, 2024	1.0	Elaboration	External Consulting
April 02, 2024	1.0	Approval	Raquel Birck – Managing Partner