

	PREVENTION POLICY MONEY LAUNDERING AND TO THE FINANCING OF TERRORISM.	CODE PL -001	
		Rev	Pág
		Nº:001	01-22
Right5 Online N.V. In the Commercial Register of the Curaçao Chamber of Commerce & Industry is registered under number 156281: Right5 Online N.V.			
Written by:Irati Aparecida Santos		Date:2024-08-15	
Reviewed by: Jarbson Santana de Jesus		Date:2024-09-03	

PREVENTION POLICY
MONEY LAUNDERING AND
TO THE FINANCING OF TERRORISM.

Content

MESSAGE FROM THE COMPANY PRESIDENT	3
I. INTRODUCTION	4
a) CONCEPT	4
b) OBJECTIVE	4
c) APPLICABILITY	4
d) Term	5
II. RESPONSIBILITIES	5
III. INTERNAL RISK ASSESSMENT	8
IV. MONITORING, SELECTION AND ANALYSIS OF OPERATIONS AND SUSPICIOUS SITUATIONS	9
V. PROCEDURES DESTINED TO GET TO KNOW CUSTOMERS	9
SAW. PROCEDURES DESTINED TO GET TO KNOW THE EMPLOYEE	10
VII. THE PROCEDURE DESTINED TO MEET PARTNERS AND SUPPLIERS	10
VIII. POLITICALLY EXPOSED PERSON - PEP	11
IX. IDENTIFICATION OF THE FINAL BENEFICIARY	13
X. COMMUNICATIONS TO COAF	14
XI. EFFECTIVENESS ASSESSMENT	15
XII. TRAINING	16
XIII. UPDATE INFORMATION AND OPERATIONS RECORDS	16
XIV. OPERATION RECORDS IN KIND	18
XV. CRITERIA FOR PROCESSING CONFIDENTIAL INFORMATION	19
XVI. GIFTS	19
XVII. DONATIONS	20
XVIII. OFFENSES	20
XIX. COMMITMENT TO POLICY	21
XX. COMPLAINTS	21
XXI. MAIN STANDARDS	21

MESSAGE FROM THE COMPANY PRESIDENT.

Dear Team,

As part of our unwavering commitment to maintaining the highest standards of integrity and compliance, we are pleased to introduce our new Prevention Policy for Money Laundering and Financing of Terrorism. This policy has been developed to ensure that our organization remains vigilant and proactive in identifying, preventing, and reporting any activities that may be related to money laundering or the financing of terrorism.

Money laundering and the financing of terrorism are serious crimes that pose significant risks not only to our organization but to the global financial system as a whole. As such, it is our collective responsibility to stay informed, vigilant, and compliant with all relevant laws and regulations.

This policy outlines the procedures and controls that will be implemented across all levels of our organization. It provides clear guidelines on identifying suspicious activities, reporting obligations, and the responsibilities of each team member in ensuring our compliance.

Training sessions will be conducted to familiarize everyone with the key aspects of this policy and to reinforce our commitment to upholding these standards. Your participation and adherence to this policy are crucial in safeguarding our organization and contributing to the global fight against these illegal activities.

Thank you for your attention to this important matter and for your continued dedication to maintaining the integrity of our operations.

Best regards,

Jarbson Santana de Jesus

I. INTRODUCTION

a) CONCEPT

According to Law 9,613, of March 3, 1998 (amended by 12,683), the crime of money laundering is characterized by the concealment or dissimulation of the nature, origin, location, disposition, movement or properties of goods, rights or values arising , directly or indirectly, of a criminal offense.

The crime process is made up of three independent phases, which can often occur simultaneously, being defined as:

- Placement: Moment at which the criminal inserts illicit resources into the financial system;
- Concealment: Phase in which the criminal seeks to break the chain of evidence, setting up an operation to give legitimacy to the money, with the aim of hiding the origin of the illegal money. Aiming to make it difficult to track resources through actions such as ghost accounts, small deposits;
- Integration: Moment when illicit money has already acquired the appearance of legitimate, that is, when resources are inserted into the economic system, such as, for example, purchasing supposedly legal assets, or investing in legal businesses.

Terrorist financing is a crime that, unlike money laundering where the intention is financial profit, criminals do not have an economic intention, but commit terrorist activities for political, religious, or ideological motivation, with the criminal act having great publicity, and not acting discreetly.

b) GOAL

This Policy reinforces the commitment of (Company Name), establishing guidelines, rules and procedures that must be observed by all employees, suppliers and other third parties linked to the institution, with the objective of promoting the adequacy of operational activities in relation to Regulations and Laws relating to the prevention of money laundering and combating the financing of terrorism.

c) APPLICABILITY

The Policy must be observed by all members of our company, including: Directors, President, Vice-Presidents, Employees, Interns, Commercial

Partners (consultants, commercial agents and partners) who act on behalf of [COMPANY NAME] and suppliers.

d) Validity

It will be valid for an indefinite period and must be reviewed and approved by the institution's Board of Directors and/or Executive Committee due to updates and changes to Laws and Regulations relating to the prevention of money laundering and terrorist financing, or possible business practices of the Prudential Conglomerate that justify the update of this Policy.

II. RESPONSIBILITIES

a) BOARD OF DIRECTORS (Responsible for the PLDFT program)

- Appoint a statutory director, responsible for complying with the standards established by CVM Instruction 50 and Bacen Circular nº 3978, in particular, for the implementation and maintenance of the PLDFT Policy;
- Approve the PLDFT Policy and monitor its applicability and compliance together with Compliance;
- The director responsible for PLDFT prepares the report relating to the internal risk assessment of LDFT, to be forwarded to the Board of Directors and board of directors;
- The responsible director must document and approve an internal assessment with the objective of identifying and measuring the risk of using products and services in the practice of money laundering and terrorist financing;
- Establish controls with the aim of preventing the risk of Money Laundering and Terrorist Financing;
- Have access to the information necessary for the proper management of PLDFT risks;
- Respond to reports of suspicious operations and/or signs of LDFT.

b) EMPLOYEES

It is the responsibility of all employees of the institution:

- Monitor operations and suspicious situations;
- Know and understand the search for ways to prevent suspicious operations and situations that may be indicative of money laundering and terrorist financing;
- Do not omit any issue pertinent to money laundering and terrorist financing;
- Know and comply with the rules that deal with the crime of PLDFT;
- Know and comply with the obligations set out in this Policy.

c) COMPLIANCE

- Develop the Policy, as well as document and disseminate it to all employees and partners of the institution;
- Approve the Policy together with the Board;
- Provide all employees and partners with periodic training programs to ensure that everyone is properly oriented and updated regarding their obligations and responsibilities in accordance with applicable standards and laws;
- Supervise the Policy and regularly check the means of combating MLFT crime that are adopted by the institution, being able to suggest the implementation of new procedures, controls and even new policies and/or manuals;
- Perform due procedure diligence of all operations involving the institution's clients;
- Be the means of communication with regulatory bodies;
- Institute processes and procedures for identifying, monitoring and analyzing activities and/or operations suspected of money laundering and terrorist financing;
- Update information about the institution and provide clarifications when necessary to COAF;
- Periodically monitor news published in the media related to the crime of LDFT;
- Analyze due diligence carried out by the Human Resources area, to grant approval or rejection in the hiring of potential employees;

- Carry out analysis of product and service projects, with the aim of preventing and mitigating possible risks arising from the practice of LDFT crimes;
- Carry out risk analysis for clients (Individuals and Legal Entities);
- Prepare mandatory reports, observing regulatory deadlines.

d) HUMAN RESOURCES

- Institute controls to assist Compliance and ensure that employees and third parties are trained annually;
- Adhere to controls to prove the knowledge of employees at the beginning of their activities;
- Carry out reputational analysis during the hiring phase;
- Seek monitoring of employees' financial situation.

e) PLDFT COMMITTEE

The Committee is the collegial, non-statutory body, of a permanent nature and with deliberative powers, regulated by its Terms of Reference, composed of professionals from the institution.

The committee's responsibilities are:

- Approve internal standards, procedures, controls, measures and guidelines related to LDFT;
- Whenever changes to policies and/or manuals related to PLDFT occur, the committee must submit them to the Board;
- Monitor the effectiveness of procedures, policies and internal controls in force at the institution;
- Analyze communications and reports that are issued by regulators, auditors, determining what is necessary to meet demands;
- Hold debates on incidents reported by the institution and the regulator;
- Decide on atypical cases identified by employees.

f) INTERNAL AND EXTERNAL AUDIT

- Carry out reviews and evaluate effectiveness and evidence regarding the implementation of the PLDFT Policy, controls, and procedures .

III. INTERNAL RISK ASSESSMENT

The institution adheres to a risk-based approach aimed at ensuring that adequate controls and means are adopted by the institution to mitigate the risks that were detected.

The internal risk assessment will seek to detect, identify and verify the risk of products and services offered by the institution regarding LDFT. Risks must be assessed regarding their probability of occurrence and the magnitude of the financial, legal, reputational and socio-environmental impacts for the institution.

As for the profiles that will be considered to analyze the risks, the following must be considered, at a minimum:

- of customers;
- of the institution, including the business model and geographic area of operation;
- operations, transactions, products and services, covering all distribution channels and the use of new technologies; It is
- of the activities carried out by employees, partners and outsourced service providers.

The risk assessment must be documented and approved by the responsible director of PLDCFT with the Central Bank of Brazil (BACEN)/Securities Commission (CVM), as well as being made available for information by the board of directors (if applicable), the institution's board of directors , risk committee and audit committee (when existing).

Regarding the frequency of reviewing the internal risk assessment, it must occur at most every two years, or when significant changes occur in the risk profiles that support such assessment, with such situations being highlighted in the operational procedures described in the specific manuals.

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

The Compliance department legal is responsible for monitoring, selecting and analyzing operations and situations that have signs of money laundering and terrorist financing. This monitoring is carried out through a specific system called Netrin.

When signaled to area After confirming or discarding the hypothesis, an analysis dossier is created and this detailed documentation is stored.

The period for carrying out the analysis procedures for selected operations and situations cannot exceed 45 days, counting from the date of selection of the operation and situation. Furthermore, every 03 months the institution has a periodic analysis established to verify the effectiveness of monitoring procedures, as well as the systems that are used.

V. PROCEDURES DESTINED TO GET TO KNOW CUSTOMERS

The procedure aimed at getting to know customers, also called “ Know your Client ”, this is a set of precise actions that aim to guarantee the identification, economic activity, and coherence of the origin, asset constitution and financial resources of clients, meaning clients, individuals and legal entities.

This process includes capturing, updating, and storing customer registration information, also including specific procedures for identifying final beneficiaries and politically exposed people.

KYC procedures assist in monitoring and maintenance with the institution's customers, covering qualification and classification, that is, adopting procedures that allow qualifying customers through collection, verification and validation of information compatible with the risk profiles and the nature of the business relationship, including with regard to the condition of the client called Politically Exposed Person and the final beneficiaries of legal entity clients.

Furthermore, the institution must classify its customers based on the risk categories defined in the risk assessment carried out, using as a basis the information obtained in the customer qualification procedures.

Furthermore, the institution is prohibited from engaging in business relationships without a correct KYC procedure having been completed. Also, the entire process that is carried out by the institution is formalized and archived in accordance with what is provided by the institution's regulators.

VI-SAW. PROCEDURES DESTINED TO KNOW THE EMPLOYEE

The “ Know your Employee ”, a procedure known as “Know your Employee”, is a set of rules, procedures carried out by the institution prior to hiring, as well as during its relationship for registration updating and monitoring, and must be done periodically.

This procedure ensures that the institution carries out adequate hiring and training of employees, enabling effective control over the financial situation and competence, preventing relationships with people involved in fraud and unethical actions.

When checking candidate information, if something is identified that is inconsistent and goes against this institution's policy and code of conduct, the Human Resources area must forward what was identified in the due diligence process. diligence for the Compliance area to analyze and grant its opinion of approval or rejection.

During the process of verifying candidate information, if any inconsistency or risk factor is identified, the recruitment area must forward the item to the Compliance area for analysis and approval. If rejected, hiring does not proceed, and if approved, the candidate's admission process continues.

VII. THE PROCEDURE DESTINED TO MEET PARTNERS AND SUPPLIERS.

The institution has a set of procedures, controls and rules that are used to identify and qualify third parties (partners and suppliers) who wish to have some type of

relationship with the company. For these third parties to be admitted, they must comply with the policy and risk assessment, as it is not the institution's desire to build ties with individuals and/or legal entities that are involved in illegitimate activities.

After carrying out an internal procedure and if it is verified that partners and/or suppliers present greater risk, the institution must adhere to additional means, such as procedures and due diligence. further diligence , and such notes must be forwarded to relevant areas and discussed in committees.

The activities of these third parties must be evaluated based on the internal risk classification, and it is mandatory that the information from these third parties is kept up to date, as well as that the institution carries out a registration update of the data, considering any changes that imply a change in classification in the risk categories .

If the institution enters into contracts and partnerships with financial institutions/correspondents located abroad, it must:

- Obtain information about the contractor that allows understanding the nature of their activity and their reputation;
- Check whether the contractor has been the subject of an investigation or action by a supervisory authority related to money laundering or terrorist financing;
- Certify that the contractor has a physical presence in the country where he is incorporated or licensed; know the controls adopted by the contractor relating to the prevention of money laundering and terrorist financing;
- Obtain approval from the holder of a position or function at a higher hierarchical level than the person responsible for hiring; It is
- Communicate the partnership agreement to the board of directors.

VIII. POLITICALLY EXPOSED PERSON - PEP

Politically exposed persons (PEP) are considered to be public agents who perform or have performed, in the last five years, in Brazil or in foreign countries, territories and dependencies, positions, jobs or relevant public functions, as well

as their representatives, family members and other people in your close relationship. In this case, we can define family members as relatives in the direct line, up to the second degree, such as the spouse, partner, partner, stepson and stepdaughter.

Must be classified as PEP:

I - holders of elective mandates from the Executive and Legislative Powers of the Union;

II - the holders of positions, in the Executive Branch of the Union, of:

a) Minister of State or equivalent;

b) Special Nature or equivalent;

c) president, vice-president and director, or equivalent, of indirect public administration entities; It is

d) Superior Management and Advisory Group (DAS), level 6, or equivalent;

III - the members of the National Council of Justice, the Federal Supreme Court, the Superior Courts, the Federal Regional Courts, the Regional Labor Courts, the Regional Electoral Courts, the Superior Council of Labor Justice and the Federal Justice Council;

IV - the 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, the Deputy Attorneys General of the Republic and the Attorneys General of Justice of the States and the Federal District;

V - the members of the Federal Audit Court, the Attorney General and the Deputy Attorneys General of the Public Prosecutor's Office at the Federal Audit Court;

VI - the presidents and national treasurers, or equivalent, of political parties;

VII - the Governors and Secretaries of State and the Federal District, the State and District Deputies, the presidents, or equivalent, of state and district indirect public administration entities and the presidents of Courts of Justice, Military

Courts, Courts of Auditors or equivalents from the States and the Federal District;
It is

VIII - the Mayors, the Councilors, the Municipal Secretaries, the presidents, or equivalent, of indirect municipal public administration entities and the Presidents of Audit Courts or equivalent of the Municipalities.

People who, abroad, are also considered politically exposed:

I - heads of state or government;

II - upper echelons politicians ;

III - holders of higher-level government positions;

IV - general officers and members of higher levels of the Judiciary;

V - senior executives of public companies; or

VI - leaders of political parties.

Senior managers of entities governed by public or private international law are also considered to be politically exposed persons.

Operations carried out with clients classified as politically exposed persons must always be considered high risk, and be analyzed carefully by the Compliance area. The institution must only initiate any relationship or continue the relationship that already exists with the client, only if internal procedures are observed .

IX. IDENTIFICATION OF THE FINAL BENEFICIARY

A final beneficiary is understood to be a natural person or natural persons who, jointly, own, control or significantly influence, directly or indirectly, a client on whose behalf a transaction is being conducted or benefits from it. The representative, including the attorney and agent, who exercises de facto command over the activities of the legal entity is also considered to be the final beneficiary.

The qualification procedures for the legal entity client must include the analysis of the chain of corporate participation until the identification of the natural person characterized as its final beneficiary, and at least the qualification procedures defined for the risk category of the entity must be applied to the natural person. client legal entity in which the final beneficiary holds a shareholding interest.

The minimum reference value of corporate participation must be established based on risk and cannot exceed 25% (twenty-five percent), considering, in any case, direct and indirect participation, and this value must be justified and documented.

This identification is necessary for customer registration approval, so the identified information will be stored and made available for monitoring the analysis of operations and suspicious situations. The information will seek to understand the structure of the property, and this information must be updated periodically.

If the institution is faced with the inability to identify the final beneficiary due to some identified particularity, the responsible area must signal the incident so that it can be evaluated by the PLDFT committee to analyze the incident, and the reasonableness of initiating the relationship with the client.

X. COMMUNICATIONS TO COAF

The Institution must report operations and situations suspected of money laundering and terrorist financing to COAF. This communication must be substantiated, recorded in a dossier, and cannot exceed a period of 45 days, counting from the date of selection of the operation or situation.

All data related to evidence and suspicions of the LDFT crime are confidential, and should not be made available to the parties involved, clients, and/or third parties .

Communications must be made by the business day following the operation or provisioning, and must be observed:

- Deposit or cash contribution or cash withdrawal operations of a value equal to or greater than \$10.000,00 USD
- Operations relating to payments, receipts and transfers of resources, through any instrument, against payment in kind, of a value equal to or greater than \$10.000,00 USD It is
- Request for provision of cash withdrawals of a value equal to or greater than \$10.000,00 USD

If no communication has been provided to COAF, the institution must send to the regulator each calendar year, within 10 working days after the end of the year, a statement attesting to the non-occurrence of operations or situations subject to communication.

XI. EFFECTIVENESS ASSESSMENT

Every year, with a base date of December 31st, the institution prepares a report evaluating the effectiveness of the procedures, which must be sent, for information, by March 31st of the year following the base date to the board of directors or, if non-existent, to the institution's board of directors. (AND IF ANY, TO THE AUDIT COMMITTEE.)

The report must contain information that describes the methodology adopted in the effectiveness assessment, the tests applied, the qualifications of the evaluators, and the deficiencies identified. It must also contain, at a minimum, the evaluation:

- Procedures aimed at getting to know customers, including the verification and validation of customer information and the adequacy of registration data;
- Monitoring, selection, analysis and communication procedures to COAF, including the assessment of the effectiveness of operation selection parameters and suspicious situations;
- Governance of money laundering and terrorist financing prevention policy;

- Organizational culture development measures aimed at preventing money laundering and terrorist financing;
- Periodic staff training programs;
- Procedures designed to get to know employees, partners and outsourced service providers; It is
- Actions to regularize notes arising from internal auditing and supervision by the Central Bank of Brazil/CVM.

XII. TRAINING

Right 5 Online N.V considers that knowledge is the best way to prevent the crime of money laundering and terrorist financing. Therefore, every 6 months training is carried out for all new employees, employees with a current employment contract and third parties.

The Compliance area will be responsible for providing periodic training to ensure that everyone is oriented and updated regarding their obligations and responsibilities with applicable standards and laws, and the Human Resources area will establish controls to assist Compliance and ensure that all are trained annually.

XIII. UPDATE INFORMATION AND OPERATION RECORDS

For the institution, completing customer registration is an extremely important process, analyzing LDFT from the perspective of prevention. The importance of registration observing internal procedures is indisputable, and that monitoring is carried out from the moment the customer formalizes a relationship with the institution, as when they have a relationship.

The information obtained from customers will be kept electronically by the institution, and in cases of need, on physical media. Each registration information

will be critically analyzed, and its update will occur according to observed risks regarding LDFT, not admitting that these updates occur for more than 1 year.

The institution must maintain a record of all operations carried out, products and services contracted, and must at least contain the following information:

- Type;
- Value, when applicable;
- Date of completion;
- Name and ID-Registration of the holder and beneficiary of the operation (in the case of a person resident or headquartered in the country; and
- Channel used.

If there are operations involving a natural person residing abroad, there is no need to register a ID, as defined by the Brazilian Federal Revenue Service, and the institution must include in the registration:

- Name;
- Type and number of the travel document and respective issuing country;
It is
- International body of which it is representative to carry out specific functions in the country, when applicable.

In situations of operations involving a legal entity with domicile or headquarters abroad, registration with the CNPJ is not required, in the form defined by the Brazilian Federal Revenue Secretariat, with the institution having to include in the registration:

- Company Name;
- Identification or registration number of the company in the respective country of origin.

In the case of operations relating to payments, receipts and transfers of resources, through any instrument, the institution must include in the records the information necessary to identify the origin and destination of the resources. The origin mentioned refers to the paying institution, drawee or sender and the person

drawn or sender of the funds, as well as the transfer or payment instrument used in the transaction.

The destination mentioned in the caput refers to the receiving institution or recipient and the person receiving or recipient of the resources, as well as the transfer or payment instrument used in the transaction. At least the following information must be included in the transaction record, when applicable:

- Name and ID or registration number of the sender or recipient;
- Name and ID or registration number of the recipient or beneficiary;
- Identification codes, in the payment settlement or funds transfer system, of the institutions involved in the operation; It is
- Numbers of the dependencies and accounts involved in the operation.

XIV. RECORDS OF IN-KIND OPERATIONS

In addition to the information provided in the topic above, the institution must register all type operations, in the case of operations:

- When using resources in kind with an individual value exceeding \$300 USD), the institution must include in the registration the name and respective ID registration number of the holder of the resources.
- For a deposit or contribution in kind of an individual amount equal to or greater than (\$10.000 USD), the name and respective registration number in the ID or Registration, as applicable, of the owner of the resources must be registered; name and respective ID registration number of the holder of the resources; and the origin of the resources deposited or contributed.
- Withdrawals, including those made by check or payment order, of an individual value equal to or greater than (\$10.000 USD) the institution must include in the registration, the name and the respective ID registration number or in the Registration, as applicable, of the recipient of the resources; the name and respective ID registration number of the holder of the resources; purpose of withdrawal; and the protocol number.

It is worth mentioning that if the client or holder of resources refuses to provide information about the origin of the resources deposited or staked, the institution must record the fact and use this information in the monitoring, selection and analysis procedure of operations and situations suspected of signs of LDFT.

In relation to client and non-client drawers, the institution must request provisioning at least three business days in advance of withdrawal operations, including those carried out by check or payment order, of an amount equal to or greater than (\$10.000 USD).

XV. CONFIDENTIAL INFORMATION TREATMENT CRITERIA

The following are common conduct criteria for all employees and business partners in relation to the treatment of confidential information:

- a) Signing a secrecy and confidentiality agreement whenever necessary before disclosing confidential information;
- b) Expose confidential information only to people essential for carrying out the project, as well as expose only information that is essential for the correct development of the activity;
- c) They must be stored securely and never shared with unauthorized third parties.
- d) You should not discuss, in person or by telephone, matters involving confidential or privileged information when you are in public places such as elevators, restaurants, taxis, airports or airplanes, as well as in virtual environments such as chat rooms, blogs, social networks and social areas of Right 5 Online B.V.

Leaking this information can cause harm to the company, as it can be used by direct competitors. These are a competitive differentiator and are part of the company's intellectual heritage.

It is worth mentioning that this commitment remains even after the end of your employment contract.

XVI. GIFTS

All employees of the institution are prohibited from giving and receiving gifts in situations that may present some type of advantage, whether for themselves or for third parties, and those with the aim of amplifying the influence of those who will receive or offer them.

We know that business relationships with customers may involve granting and receiving gifts and meals. Therefore, it is permitted to give and receive gifts with a maximum value of up to (\$200 USD).

XVII. DONATIONS

We do not allow any type of political donation, whether donations to parties or candidates. In cases of eventualities, employees must contact the Compliance area so that the donation can be analyzed.

Furthermore, the institution and its employees are prohibited from making charitable donations to investors, whether they are potential investors or already active clients, including their affiliates.

XVIII. VIOLATIONS

Any violation of the Policy may generate consequences such as civil and criminal penalties for those responsible and employees involved. Also, sanctions will be applied to violations of this policy, which may vary between: warning, suspension, dismissal from the company, among other sanctions that the Ethics Committee deems applicable to the case. The duties of the Ethics Committee are:

- a) Clarify doubts regarding the principles contained in the Policy;
- b) Support managers in interpreting and forwarding solutions to situations that constitute violations of the Policy;
- c) Guarantee the anonymity of reports that arrive under these conditions;
- d) Analyze any situation outside of moral and ethical standards and possibly, even if not foreseen in the Policy ;
- e) Review the Policy annually and update it whenever necessary.

XIX. COMMITMENT TO POLICY

From the implementation of this Policy, and in all its revisions, all its recipients are obliged to sign a statement attesting that they have read each version of the Anti-Money Laundering and Terrorism Financing Policy.

XX. COMPLAINTS

If you witness any act contrary to our PLDFT Policy, you must report it via the Reporting Channel, via legal@right5.online or directly with the ethics committee/PLDFT.

Date of last update of this Policy: 2024-08-15

XXI. MAIN STANDARDS:

- **Law No. 9,613, of March 3, 1998, amended by Law No. 12,683, of 2012**

Provides for crimes of “laundering” or concealment of assets, rights and values; preventing the use of the financial system for illicit activities and making the criminal prosecution of money laundering crimes more efficient.

- **Law No. 13,260, of March 16, 2016**

Regulates the provisions of section XLIII of art. 5th of the Federal Constitution, regulating terrorism, dealing with investigative and procedural provisions and reformulating the concept of terrorist organization; and amends Laws No. 7,960, of December 21, 1989, and 12,850, of August 2, 2013.

- **Circular nº 3,978, dated 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 with a view to preventing the use of the financial system to commit crimes of

“laundering” or concealment of assets, rights and values, covered by Law No. 9,613, of March 3, 1998, and terrorist financing, provided for in Law No. 13,260, of March 16, 2016.

- **CVM Resolution No. 50, of August 31, 2021**

Provides for the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction - PLD/FTP within the scope of the securities market and revokes CVM Instruction No. 617, of December 5, 2019 and the Explanatory Note to CVM Instruction No. 617, of December 5, 2019.

- **Circular Letter No. 4,001, dated January 29, 2020**

Discloses a list of operations and situations that may constitute evidence of the occurrence of crimes of "laundering" or concealment of assets, rights and values, as covered by Law No. 9,613, of March 3, 1998, and financing of terrorism, provided for in Law No. 13,260, of March 16, 2016, subject to communication to the Financial Activities Control Council (COAF).

- **Coaf Resolution No. 36, of March 10, 2021**

Regulates the adoption of policies, procedures and internal controls to prevent money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction that allow compliance with the provisions of arts . 10 and 11 of Law No. 9,613, of March 3, 1998, by those who are subject, under the terms of its art. 14, § 1, to the supervision of the Financial Activities Control Council - COAF.

Irati Santos

