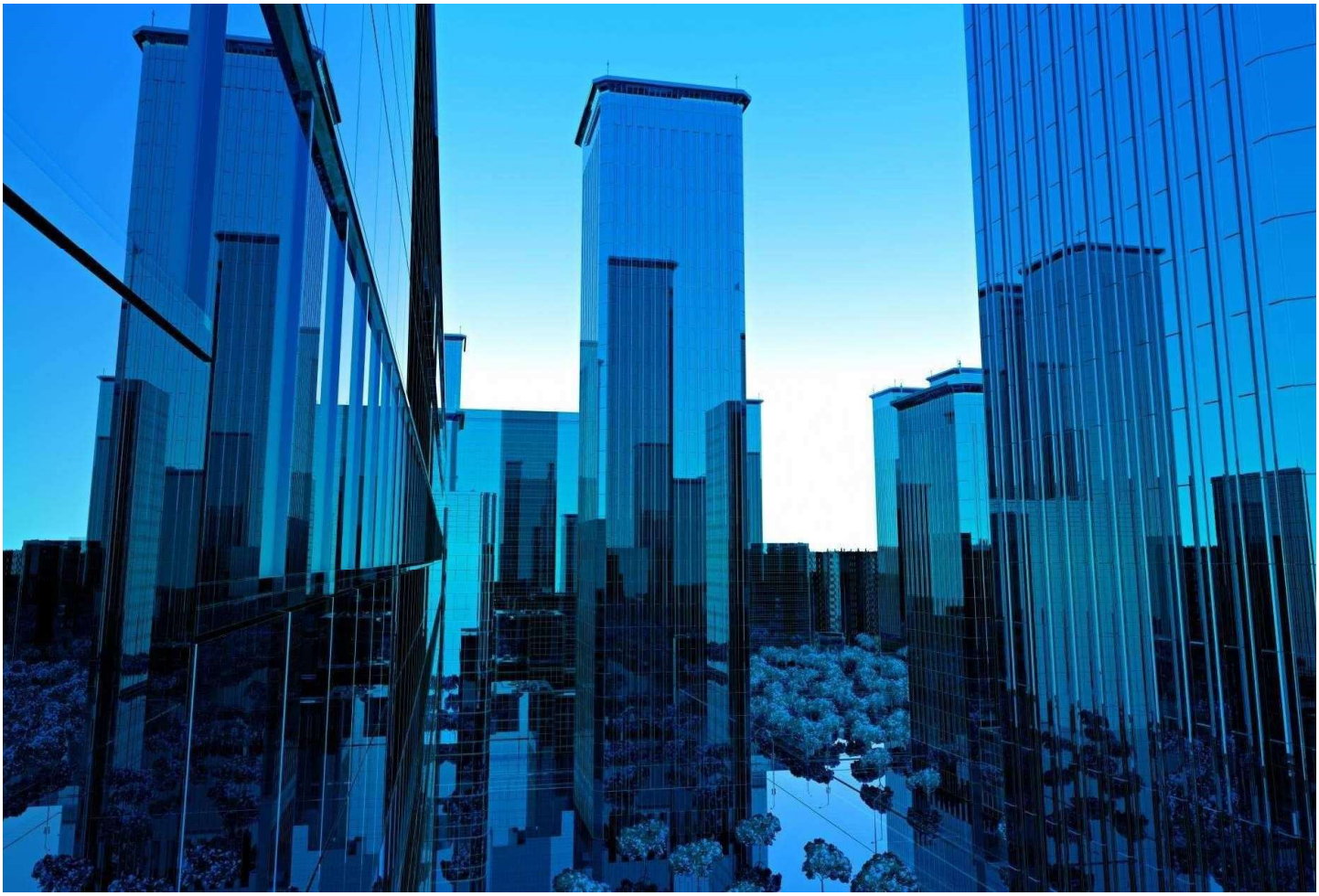

BANCO FIBRA

POLICY FOR THE PREVENTION OF MONEY LAUNDERING, TERRORIST FINANCING, AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION – AML/CTF

1. DEFINITION

This policy aims to define, for employees, partners, suppliers, and third party service providers, the guidelines and best practices for the prevention and combat of money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction ("AML/CTF") at Banco Fibra S.A. and its subsidiaries, reinforcing its commitment to clients and society in combating such crimes, in accordance with current regulatory requirements.

Additionally, this policy was developed based on Banco Fibra's Internal Risk Assessment ("IRA"), to establish criteria and procedures compatible with the risk profiles of clients, the institution, operations, transactions, products and services, as well as employees, partners, suppliers, and third party service providers.

2. TARGET AUDIENCE

- Banco Fibra, its subsidiaries, and its Cayman Branch (collectively referred to as "Banco Fibra" or the "Bank" in this document).

3. DESCRIÇÃO

- **Money Laundering**

The term "money laundering" refers to the act of concealing the criminal origin of assets, funds, and capital, with the intent of reintroducing them into the formal economy under the appearance of legality. Given the seriousness of this conduct, and in line with international best practices, brazilian law establishes penalties for those who engage in the concealment or disguise of the nature, origin, location, disposition, movement, or ownership of assets, rights, or values derived, directly or indirectly, from a criminal offense. The same penalty applies to individuals who, with the intent to conceal or disguise the use of assets, rights, or values derived from a criminal offense, perform the following acts: (i) conversion into lawful assets; (ii) acquisition, receipt, exchange, negotiation, provision or receipt as collateral, custody, deposit, movement, or transfer; (iii) import or export of goods with values that do not correspond to their true worth; (iv) use of assets, rights, or values derived from a criminal offense in economic or financial activities; and (v) participation in

a group, association, or office, with knowledge that its primary or secondary activity is aimed at committing crimes as defined by current legislation.

- **Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction**

Terrorism consists of the practice, by one or more individuals of the acts described below, motivated by xenophobia, discrimination, or prejudice based on race, color, ethnicity, or religion, when committed with the intent to provoke social or widespread terror, endangering individuals, property, public peace, or public safety. Acts of terrorism include: (i) using or threatening to use, transporting, storing, carrying, or possessing explosives, toxic gases, poisons, biological, chemical, nuclear substances, or other means capable of causing harm or mass destruction; (ii) sabotaging the operation of or seizing, through violence, serious threat to individuals, or by using cyber mechanisms, full or partial control, even if temporary, of communication or transportation systems, ports, airports, train or bus stations, hospitals, healthcare facilities, schools, sports stadiums, public facilities or locations where essential public services operate, energy generation or transmission facilities, military installations, oil and gas exploration, refining and processing facilities, and banking institutions and their service networks; (iii) attacking the life or physical integrity of a person.

Additionally, as defined by a United Nations Security Council Resolution, States are obligated to halt any action aimed at supporting non-state actors in the development, acquisition, production, possession, transport, transfer, or use of nuclear, biological, and chemical weapons and their delivery systems. This strategy outlines a series of specific measures to combat terrorism in all its forms, at national, regional, and international levels.

Therefore, governments, through their institutions, must require activities that identify and adopt measures to mitigate the risks of financing the proliferation of weapons, in addition to money laundering and terrorism.

- **Scope and Application of Sanctions**

Brazilian law stipulates severe penalties for anyone who offers or receives, obtains, stores, keeps in deposit, requests, invests, or in any way contributes to the acquisition of assets, goods, or financial resources with the purpose of financing, in whole or in part, an individual, group of individuals, association, entity, or criminal organization whose primary or secondary activity, even if occasional, involves the commission of the crimes outlined above.

Banks and other financial agents, as defined by current legislation, including their representatives and employees, must have mechanisms in place to prevent money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction, by hindering, preventing, and/or reporting the occurrence or suspicion of illicit activity.

In this regard, employees of the Bank, its subsidiaries, partners, suppliers, and outsourced service providers who are negligent, omissive, or complicit in money laundering, terrorist financing, or the financing of weapons of mass destruction are subject to administrative and civil sanctions, regardless of the role they perform within the Bank.

It is the responsibility of Management and of each employee, partner, and outsourced service provider to comply with laws and regulations related to ML/TF crimes. If they become aware of any breach of the guidelines set forth in this policy, or of any suspicious operations, they must immediately inform the Compliance & Sustainability area via the email compliance.pld@bancofibra.com.br.

3.1 Institutional Guidelines

The processes and controls carried out for the execution of operations and services by Banco Fibra are supported by the Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing Program ("AML / CTF"), whose guidelines must be observed by all those acting on behalf of the Bank and its subsidiaries:

- Prevent the practice of AML / CTF in the conduct of Banco Fibra's business in Brazil and abroad, in accordance with national legislation, as well as the laws in force in the countries where it operates;
- Strictly observe compliance with the AML / CTF policy, ensuring proper implementation of procedures and controls, as well as identification and correction of any deficiencies found;
- Perform duties involving relationships with clients, employees, partners, suppliers, and outsourced service providers in accordance with the internal guidelines and procedures for the prevention, detection, and combat of corruption and fraud established in Banco Fibra's Integrity Program. The scope of the program defines essential principles for the functioning and effectiveness of the activities currently managed and monitored by the Compliance & Sustainability department, including, in particular, the scope of Law No. 12.846 / 13, as amended (Anti-Corruption Law);
- Act in accordance with the international commitments assumed by the Brazilian federal government regarding the prevention and combat of AML / CTF;
- Encourage and participate in joint actions within the national and international financial system to prevent and combat AML / CTF and corruption crimes;
- Identify, qualify, and classify clients, and keep their registration information up to date;
- Do not initiate business relationships without the satisfactory completion of client identification, qualification, and classification procedures;
- Maintain consolidated internal controls and records that allow verification of proper client identification, qualification, and classification, as well as compatibility between resource movements, economic activity, and financial capacity;

- Do not allow the movement of funds through anonymous accounts or accounts linked to fictitious holders;
- Maintain records of all operations involving domestic or foreign currency, securities, metals, or any other asset convertible into cash;
- Maintain internal control procedures to detect operations that indicate signs of AML / CTF crimes;
- Adopt procedures aimed at inhibiting AML / CTF crimes in the development and review of products and services, including the adoption of new technologies;
- Conduct, every two years or when significant changes in risk profiles occur, the Internal Risk Assessment ("IRA") to identify and measure the risk of the Bank's products and services being used for money laundering and terrorism financing;
- Carry out Effectiveness Assessments of internal processes related to AML / CTF, including evaluation of policies, procedures, and internal controls;
- Classify clients (Know Your Customer – KYC), candidates and employees (Know Your Employee – KYE), and partners (Know Your Partner – KYP), including outsourced service providers and other partner categories, according to the risk categories defined for each modality and in accordance with the IRA;
- Use parameters established in current regulations for transaction recording and identification of transactions considered indicative of AML / CTF, in the development or acquisition of automated transaction monitoring systems;
- Carefully analyze the instruments used, usage channels, execution methods, parties and values involved, financial capacity, client's economic activity, nature and purpose, and any indication of irregularity or illegality involving the client or their operations, especially in the analysis of transactions suspected of AML / CTF;
- Report to the competent authorities, within the deadlines and formats required by applicable legislation, operations or proposed operations that, under regulations, indicate signs of AML / CTF;
- Carry out, confidentially, including in relation to clients, the processes of recording, analyzing, and reporting to competent authorities operations or movements considered suspicious or that meet the criteria for mandatory reporting defined in current regulations;
- Adopt restrictive measures regarding clients, employees, partners, suppliers, and outsourced service providers, preventing the execution of business, services, or operations when circumstances reveal evidence / signs of AML / CTF or corruption;
- Maintain correspondent relationships only with other financial institutions that have controls and mechanisms for AML / CTF prevention and anti-corruption;
- Adopt criteria for hiring and conduct of employees, focusing on AML / CTF prevention and anti-corruption, through the Know Your Employee procedure;
- Adopt criteria for hiring and conduct of partners, suppliers, and outsourced service providers acting on behalf of the institution, focusing on AML / CTF prevention, through the KYP procedure;
- Maintain a specific training program for employees and relevant outsourced service providers.

3.2 AML/CFT Procedures

The AML/CFT Program of Banco Fibra consists of a set of control measures, as detailed below:

- **Internal Risk Assessment ("IRA") –** This procedure is conducted by the Compliance & Sustainability department, based on the Risk-Based Approach ("RBA") adopted by the institution, in order to identify AML/CFT risks, considering the following risk profiles: (i) clients; (ii) the institution and its business model / geographic area of operation; (iii) operations, transactions, products and services, including distribution channels and the use of new technologies; and (iv) activities carried out by employees, partners, suppliers, and outsourced service providers.

  The IRA also considers risk categorization based on its probability and financial, legal, reputational, and socio-environmental impacts on the Bank. It must be reviewed at least every two (2) years, or whenever there are significant changes in the risk identification process. Additionally, when available, assessments conducted by public entities in the country regarding AML/CFT risk are used as supporting inputs for the IRA.

  According to this methodology and as a result of the assessment, all clients conducting transactions with the Bank will be classified into one of the following risk categories: Very Low, Low, Medium, High, and Very High, and must be subject to identification, qualification, and monitoring criteria, as applicable, as well as approval in accordance with the authority levels defined in 01-07-06/1 NI Know Your Client.

  Furthermore, partners, including suppliers and outsourced service providers, and other partner categories will be classified into the following risk categories: High, Medium, and Low, and must be subject to identification, qualification, and monitoring criteria, as well as approval in accordance with the authority levels defined in 01-07-24/1 NI Know Your Partner.

  Employees, including candidates participating in recruitment processes, will be classified into High, Medium, and Low Risk categories, according to the guidelines formalized in 01-14-07/1 NI Know Your Employee, and are also subject to identification, qualification, and monitoring criteria as per the internal Know Your Employee policy.

  Risk is dynamic, and therefore, any of the classifications above may be changed based on new facts or due diligence during the Bank's relationship, in accordance with the criteria and authority levels set forth in the Bank's internal policies.

- **Know Your Client ("KYC") –** This procedure is established by regulatory authorities and defines that financial institutions and their equivalents must implement a set of appropriate rules and

procedures to identify and qualify their clients, as well as to understand the origin and structure of their assets and financial resources.

Through the adoption of specific procedures in this regard, Banco Fibra aims to guide and standardize the initiation, maintenance, and monitoring of relationships with clients who use or intend to use the institution's products and services, to prevent any form of involvement in money laundering (ML) / terrorist financing (TF) or other illicit activities.

Therefore, the Know Your Client procedures seek to ensure, to the best of the Bank's efforts and at any time, the client's identity ("*who they are*"), activity ("*what they do*"), and consistency in the origin and movement of funds, whether the clients are individuals or legal entities, permanent or occasional.

Enhanced measures must be adopted for clients classified in higher risk categories, including shorter KYC validity periods and inclusion of the client in the Bank's special monitoring list.

- **Client Registration –** Client registration is one of the pillars of the Know Your Client (KYC) process and, therefore, an essential procedure for the prevention and combat of Money Laundering (ML) and Terrorist Financing (TF).

  Client registration is carried out according to the characteristics of the relationship, in compliance with current regulations. It includes the collection of registration information directly from clients, as well as from public and private database sources, the evaluation of documents and identification and qualification information, and is built upon the continuous and systematic updating of data in a secure and reliable information base.

  Client registration is a key element for the prevention and combat of ML/TF. The client's registration file serves as an important resource for transaction analysis and must include the identification of ultimate beneficial owners, that is, the natural person who ultimately, directly or indirectly, owns, controls, or significantly influences the entity, in the case of legal entities.

  The Bank has systems responsible for collecting, updating, and storing information related to identifying clients appropriately for their intended purpose. Further details regarding the client registration procedure, as well as the frequency of updates for active client records, can be found in 01-12-06/1 NI Opening and Maintenance of Registration Documents and 01-07-06/1 NI Know Your Client, both available on the Bank's intranet.

- **Client Classification (AML/CFT Rating) –** At the beginning of the relationship or upon renewal of the KYC validity period, all clients must undergo AML/CFT risk classification through the completion of the KYC form. Based on a combined assessment of registration data, relationship with the institution, geographic location, identification of PEPs, reputational checks, restrictive and sanctions lists, and the percentage of ultimate beneficial owner identification, clients will be categorized into one of the following risk levels: Very High, High, Medium, Low, or Very Low, in accordance with the Internal Risk Assessment (IRA).For risk classification purposes, the methodology considers the business relationship with the highest propensity for AML/CFT risk, as defined by the IRA. The monitoring measures, enhanced oversight, and KYC validity period are determined according to the final assessed risk classification.

  Client approvals within the KYC process must be carried out in accordance with the authority levels described in the NI Know Your Client policy.

- **Foreign Exchange Transactions** – Banco Fibra applies enhanced due diligence for clients conducting foreign exchange transactions, to prevent irregularities that may constitute criminal offenses or activities related to Money Laundering (ML) and Terrorist Financing (TF). To this end, the institution has implemented controls, including system-based tools, that ensure the regularity, economic and legal justification of the transaction, and the client's financial capacity.

- **Politically Exposed Persons (PEP) –** Banco Fibra has specific procedures for identifying Politically Exposed Persons (PEPs), either through self-declared information provided directly by the client or through independent research conducted by the Compliance & Sustainability department using PEP databases. Additionally, for initiating and maintaining relationships with clients classified as PEPs, the client acceptance procedures include consideration of the presence of PEPs within the corporate structure. This factor is treated as a risk variable in the AML/CFT assessment and, therefore, influences the final risk classification.

  The Compliance & Sustainability department conducts enhanced monitoring for all clients classified as PEPs, or for transactions involving a PEP and/or related parties, in accordance with applicable legislation.

  Companies whose ownership or management includes individuals identified as PEPs will also be classified as such (expanded PEP concept) and must follow the same monitoring and risk classification guidelines as clients identified as PEPs.

  The categories of positions and conditions eligible for PEP classification are detailed in 01-07-06/2 GP Know Your Client.

- **Monitoring, Selection, Analysis, and Reporting ("MSAR")** – Banco Fibra conducts ongoing monitoring of financial transactions and operations carried out by its clients, identifying situations that may indicate signs of Money Laundering (ML), Terrorist Financing (TF), or other occurrences subject to reporting to the Financial Activities Control Council ("COAF") or to the respective competent authorities in the international jurisdictions in which it operates. The monitoring process involves routines and criteria for selection and analysis, supported by specific rules to comply with current regulations, through automated procedures using systems provided by specialized vendors. Alerts are assessed by the Compliance & Sustainability department to determine whether reporting is applicable, except in cases that do not fall within the scope of mandatory reporting, as defined in 01-07-17/2 GP AML/CFT Prevention Policy.

  The monitored information is confidential and restricted to the Compliance department, which is responsible for defining processes and controls, as well as for storing client files for the minimum period required by applicable regulations, for presentation to auditors and regulatory authorities.

- **Cash Transactions** – Although the institution does not have an active structure for handling cash transactions, whether in local or foreign currency, as defined in its business model, it is important to note that the monitoring mentioned above includes, as a preventive measure, transactions of this nature. The Compliance & Sustainability department has configured specific rules in the monitoring system for such cases, including cash movements, increases in the number of cash deposit transactions, or volumes exceeding the limits established by the Central Bank of Brazil.

  In cases involving the receipt of checks, the information must be previously submitted by the Operations department, through the Branch and Judicial Orders area, for proper analysis by the Compliance & Sustainability department. When necessary, the case is forwarded to the Compliance, AML/CFT, and Social, Environmental, and Climate Risk Committee for deliberation.

- **Reporting of Fraud and Suspicious Transactions** – All transactions or transaction proposals that, based on the parties involved, amounts, execution methods, and instruments used, may indicate suspicious activity—or that meet the conditions established by current regulations—must be reported to COAF and to the competent Regulatory Authorities in the jurisdictions where the Bank operates, when applicable. Suspicious cases related to ML / TF must be submitted to the deliberation process of the Compliance & Sustainability department (as defined below) and, when applicable, to the analysis of the Compliance, AML / CFT, and Social, Environmental, and Climate Risk Committee. The decision to report or not must be formalized in meeting minutes, and if the decision is to report, the deadline is up to one (1) business day following the reporting decision.

The following guidelines must also be observed for communications to COAF or to the competent Regulatory Authorities in the jurisdictions where the Bank operates:

- The identity of the employee reporting any suspicious ML / TF transaction must be preserved;
- The Compliance & Sustainability department is ultimately responsible for registering the occurrence with COAF or an equivalent system, or with the Regulatory Authority / Competent Authority, depending on the nature of the transaction;
- The Compliance & Sustainability department operates independently in the process of reporting fraud and suspicious transactions;
- Communications must be made without the knowledge of the parties involved or any third parties; and
- The client or potential client must not be notified or informed about the report.

The timeframe for executing monitoring and selection procedures for suspicious transactions or situations must not exceed forty-five (45) days from the date of the transaction or occurrence.

COAF conducts a monthly monitoring procedure via SISCOAF to analyze the statistics of submitted reports, aiming to ensure that communications to the Regulatory Authority are always appropriate and effective ("Scores assigned by COAF"). To verify the scores assigned to the Bank, the Compliance & Sustainability department accesses the SISCOAF system monthly and checks for any scores related to Banco Fibra's reports. Based on these scores and any issues raised by COAF, improvement actions may be implemented for future communications.

If no reports have been submitted to COAF by the end of the current year, the Compliance & Sustainability department must, within the first ten (10) business days of January, submit a notification of absence of communications, including for its subsidiaries, when applicable.

- **Know Your Partner ("KYP") –** The KYP procedure applies to partners, suppliers, and outsourced service providers, whether categorized as relevant or not, and must be carried out prior to the start of the relationship or during registration renewal. This is done through the completion of the Know Your Partner form, applicable to the type of relationship (Supplier, Relevant Supplier, Brokers, and other partner categories defined in 01-07-24/1 NI Know Your Partner). Topics related to AML/CFT and anti-corruption are addressed both before the relationship begins and during periodic registration renewal. The purpose of this procedure is to avoid any type of relationship with counterparties that are unfit or suspected of involvement in illicit activities, such as corruption, money laundering, terrorist financing, financing of weapons of mass destruction, environmental or social harm, or

climate-related risks, and to ensure that such parties have appropriate AML/CFT procedures in place, when applicable.

The Know Your Partner procedure must include AML/CFT risk assessment by the Compliance & Sustainability department for partners, suppliers, and outsourced service providers, as well as other partner categories, in accordance with the IRA and the procedures described in specific policies. The partner must be classified into High, Medium, or Low risk levels, based on the completion of the "Third Party Service Provider Registration Form and *Due Diligence Questionnaire*," filled out and signed by the third party. The information, combined with Compliance research, will support the risk classification.

Additionally, the Compliance & Sustainability department may conduct due diligence visits with support from the Procurement team when evaluating partners, suppliers, and outsourced service providers, or with support from the Commercial team when evaluating brokers.

Moreover, partners, suppliers, and outsourced service providers of the Bank and its subsidiaries may report, via the Alô Ética Channel, any situations indicating potential wrongdoing of any nature related to Banco Fibra's activities. This includes acts that contradict the ethical standards adopted and promoted by Banco Fibra, such as corruption, internal or external fraud, in accordance with the procedures defined in 01-07-25/1 NI Alô Ética Channel Regulation.

- **Know Your Employee ("KYE") –** Banco Fibra maintains mechanisms for collecting registration data, verification, identification, and classification of employees prior to hiring (candidates in recruitment processes), aiming to gather information related to conflicts of interest, reputation, registration details, among others. Additionally, at the time of hiring, each employee must sign the Code of Ethics and Conduct Adherence Term, as well as complete and sign the Conflict of Interest Statement, which must be updated by the employee whenever any new relevant fact arises, in accordance with the procedures detailed in the NI Know Your Employee.

  The KYE procedure, conducted by the Compliance & Sustainability department, includes AML/CFT risk assessment for candidates applying for permanent or internship positions at Banco Fibra, in accordance with the IRA and the procedures described in specific policies. Candidates must be classified as High, Medium, or Low Risk.

  Furthermore, the Compliance & Sustainability department performs an annual monitoring of the active employee database to identify potential changes in risk level. These cases must be reassessed by the appropriate authority levels, in accordance with the guidelines formalized in 01-14-07/1 NI Know Your Employee.

It is the responsibility of each department manager to immediately report to the Compliance & Sustainability department, via the email compliance.pld@bancofibra.com.br, any situations that may indicate significant changes in the employee's socioeconomic profile, repeated non-compliance with internal AML/CFT policies, or behavioral changes that may represent a risk factor to the Bank.

Additionally, employees may report, via the Alô Ética Channel, any situations indicating potential wrongdoing of any nature related to Banco Fibra's activities. This includes acts that contradict the ethical standards adopted and promoted by Banco Fibra, such as corruption, internal or external fraud, in accordance with the procedures defined in 01-07-25/1 NI Alô Ética Channel Regulation.

- **Evaluation of New Products and Services –** New products and services shall be evaluated in advance by the Compliance & Sustainability department from an AML/CFT perspective, in accordance with the guidelines established in the internal policy for Product and Service Development. The result of the analysis will be recorded in the Product Approval Form ("PAF").

- **New Technologies –** The use of new technologies shall be evaluated in advance by the Compliance & Sustainability department, to identify AML/CFT risks related to their intended purpose, as well as to assess the service provider, when applicable.

- **Effectiveness Assessment –** The effectiveness assessment shall be carried out by the Bank's Internal Controls and Operational Risk department and must cover the effectiveness of this policy, as well as the procedures and controls established for AML/CFT.

  The assessment must also consider the adequacy of the controls implemented to ensure compliance with the AML/CFT policy, as well as the evaluation of: (i) procedures related to KYC, including client registration; (ii) procedures for monitoring, selection, analysis, and reporting to COAF, including the effectiveness of the parameters used for identifying transactions and suspicious situations; (iii) AML/CFT governance; (iv) initiatives to promote an AML/CFT-oriented organizational culture; (v) periodic employee training programs; (vi) procedures for knowing employees, partners, suppliers, and outsourced service providers; and (vii) remediation actions for findings issued by Internal Audit, the Central Bank of Brazil, and other regulatory authorities.

  The report resulting from the Effectiveness Assessment must be produced annually and include the evaluation results and action plans proposed for the identified findings. It must be submitted by March 30 of each year to the Audit Committee (COAUD) and the Board of Directors for their awareness.

The action plans proposed in response to the findings from the Effectiveness Assessment shall be monitored by the Internal Controls department until their full implementation. A Follow-up Report must be formalized by June 30 of each year and submitted for review by the Executive Board, COAUD, and the Board of Directors.

- **AML/CFT Systems –** Market systems are used to carry out the necessary controls and procedures for AML/CFT, including background checks, screening of restrictive and sanctions lists, PEP verification, and searches for negative media related to financial crimes, ML/TF, social, environmental, and climate risks, among others. Additionally, KYC analyses and corresponding risk classifications are recorded in a system specifically designed for this purpose.

- **Other AML/CFT Procedures –** Banco Fibra conducts due diligence and preliminary assessments of counterparties not covered by the KYC, KYE, or KYP processes, such as potential buyers of assets from BNDU sales or assignees of transactions registered under Credit Restructuring. Transactions must only be carried out with reputable individuals or institutions, and any cases deemed suspicious must be reported to COAF or the respective applicable authorities.

3.3. Training

The dissemination of concepts related to ML/TF crimes and the commitment of Senior Management and all employees are fundamental conditions for the success of actions aimed at preventing and combating ML/TF.

To achieve this objective, Banco Fibra has a training, update, and information dissemination program focused on the prevention of ML/TF crimes, directed at all employees.

The training sessions must ensure that employees are able to identify situations that may indicate signs of ML/TF crimes and report them to the department responsible for evaluation and communication to the competent authorities.

Training must be conducted at least once a year and is mandatory for all new employees upon hiring.

The People & Culture department is responsible for generating electronic alerts and sending them to employees with pending training. If an employee fails to complete the training after receiving alerts, this information must be reported to the Compliance & Sustainability department.

3.4 Assignment of Responsibilities

- **Board of Directors**
  - Approve the annual review of this policy; and
  - Receive and approve the annual report resulting from effectiveness testing, as well as monitoring the implementation of action plans proposed for identified risks.

- **AML/CFT Director**
  - Promote AML/CFT culture among employees, partners, suppliers, and outsourced service providers, as applicable, including the adoption of periodic training programs;
  - Monitor compliance with the AML/CFT policy, rules, procedures, and controls, as well as their updates, to ensure proper risk management;
  - Enforce disciplinary actions against employees, partners, suppliers, and outsourced service providers who fail to comply with AML/CFT procedures;
  - Supervise the AML/CFT department and the Compliance, AML/CFT, and Social, Environmental, and Climate Risk Committee;
  - Have broad, unrestricted, and timely access to any information related to the Bank's operations, enabling the acquisition of necessary data for fulfilling their responsibilities and those of their team, especially regarding effective ML/TF risk management;
  - Allocate appropriate resources for maintaining and improving the AML/CFT program; and
  - Ensure the AML/CFT program is regularly reviewed to maintain its efficiency and effectiveness, incorporating new risk factors when applicable.

- **Compliance, AML/CFT, and Social, Environmental, and Climate Risk Committee**
  - Monitor the Integrity Program, ensuring the dissemination of integrity standards and ethical conduct as part of the institution's culture;
  - Ensure proper management and communication of the Compliance Policy to employees and third parties, as well as the effectiveness and continuity of the procedures, principles, and guidelines established in the policy;
  - Recommend corrective measures when non-compliance with the Compliance Policy procedures and guidelines is identified;
  - Evaluate cases involving clients, partners, suppliers, or outsourced service providers analyzed by AML/CFT Compliance that show signs of crimes or irregularities requiring higher-level decisions; and
  - Evaluate cases involving clients, partners, or outsourced service providers analyzed by Compliance regarding Social, Environmental, and Climate Risks that require higher-level decisions.

- **Compliance & Sustainability Department**
  - Promote the implementation, maintenance, and updating of governance, rules, and procedures related to the Bank's AML/CFT framework, including Know Your Client (KYC), Know Your Employee (KYE), Know Your Partner (KYP), and the monitoring, selection, analysis, and reporting of suspicious activities related to ML/TF;
  - Ensure, together with Senior Management, the existence, updating, and enforcement of internal control guidelines, policies, and procedures for AML/CFT;
  - Monitor the adequacy of the AML/CFT program;
  - Operate independently and autonomously to avoid conflicts of interest;
  - Ensure the prevention, detection, and reporting of transactions that may indicate crimes as defined by current legislation;
  - Have full access to all necessary information to carry out AML/CFT risk governance;
  - Promote AML/CFT culture among employees and service providers, as applicable, including through periodic training programs and communication initiatives on AML/CFT and anti-corruption, to foster and maintain a culture of integrity within the organization;
  - Interact with regulatory and self-regulatory bodies on AML/CFT-related matters;
  - Immediately and without prior notice to sanctioned parties, comply with measures established in United Nations Security Council (UNSC) sanction resolutions or designations by its sanctions committees that determine asset freezes;
  - Adopt procedures to address any non-compliance or failures identified in the AML/CFT program and report them to Senior Management based on the assigned risk level, through operational risk event reporting, as defined in the Internal Controls and Operational Risk policy;
  - Recommend to the Compliance, AML/CFT, and Social, Environmental, and Climate Risk Committee the termination of client relationships initiated by the Bank whenever ML/TF or reputational risks are identified; and
  - Maintain confidentiality of data and information, in accordance with special legislation, related to indications of ML or asset concealment crimes and terrorist financing, which must not be recorded in the database of suspected fraud attempts, as per current regulations.

- **Internal Controls Department**
  - Conduct annual effectiveness testing of the AML/CFT policy, procedures, and internal controls;
  - Monitor and provide governance for any action plans resulting from effectiveness testing; and
  - Record operational risk events related to AML/CFT and monitor the implementation of proposed remediation plans.

- **Commercial Department**
  - Ensure relationships are maintained only with reputable clients, applying all efforts to conduct proper registration and KYC procedures; and

- Immediately report to the Compliance & Sustainability department any client behavior that may suggest ML/TF-related acts or that contradict the Integrity Program.

- **All Employees**
  - Comply with AML/CFT policies, rules, procedures, and internal controls, accessing internal policies and process guides as needed, and regularly completing training available on the Bank's intranet; and
  - Promptly report any indication of ML/TF, corruption, or fraud to the Compliance & Sustainability department or via the Alô Ética Channel.

- **Partners, Suppliers, or Third Party Service Providers**
  - Comply with the applicable guidelines described in this policy; and
  - Promptly report any indication of ML/TF, corruption, or fraud to the Alô Ética Channel related to Banco Fibra's activities.

3.5 Information Maintenance

The maintenance of client registration records shall be carried out either physically or electronically, based on the documents required in the Client Registration Opening and Maintenance Policy (NI), stored in a dedicated and protected file.

For employees, partners, suppliers, or outsourced service providers, registration records shall be maintained in accordance with the policies that establish the guidelines for Know Your Employee (KYE) and Know Your Partner (KYP), respectively.

It is important to emphasize that adherence to the principles of Know Your Client (KYC), Know Your Partner (KYP), and Know Your Employee (KYE), as well as the documentation requirements, must be applied according to the risk profile of each client, service provider, or employee, as applicable.

3.6 Other Responsibilities

The guidelines set forth in this policy are also applicable to Banco Fibra's service provision in the capacity of custodian, distributor, or sub-custodian.

4. COMPLIANCE DELIBERATION

The Compliance deliberation process is carried out in cases that require higher-level decision-making but do not require review by the Compliance, AML/CFT, and Social, Environmental, and Climate Risk

Committee. The responsibility for analysis and deliberation lies with the Compliance Management, in conjunction with the Director responsible for AML/CFT.

- **Applicable evaluations within the Compliance Deliberation process:**
  - Reporting to COAF cases whose circumstances are specified in current legislation;
  - Other Compliance matters that do not require review by the Compliance, AML/CFT, and Social, Environmental, and Climate Risk Committee.

All decisions made by the department and/or the Committee must be formalized in meeting minutes and retained for a period of ten (10) years.

5. ASSET FREEZING

The Compliance & Sustainability department is responsible for monitoring asset freezing determinations issued by the United Nations Security Council (UNSC), as well as for reviewing any relevant information to ensure proper compliance—both at the beginning or renewal of client relationships through the KYC procedure, and during the monitoring of financial transactions throughout the client's relationship with the Bank.

The Compliance & Sustainability department performs daily monitoring using a market system that checks all active clients against names subject to asset freezing, based on sanction lists that include individuals, legal entities, and organizations sanctioned under UNSC resolutions or designations by its sanctions committees. These lists are updated by the provider whenever records are added or removed, and the Compliance & Sustainability department is responsible for periodically verifying the integrity of the list data.

If a client is identified as falling under these conditions, the Compliance & Sustainability department must notify the Operations and Credit Monitoring departments, which will immediately block the assets in the Dashboard system, enabling the freeze across all Bank systems using the status: "UNSC Freeze – United Nations Security Council."

The Compliance & Sustainability department will also immediately report the existence or emergence of assets belonging to clients, subject to UNSC freezing determinations to the following authorities via their respective communication channels:

- Central Bank of Brazil, via the BC Correio system;
- COAF, via the system already used for reporting; and
- Ministry of Justice and Public Security (MJSP), via the email csnu@mj.gov.br.

Any additional information required to comply with UNSC asset freezing measures will be monitored by the Compliance & Sustainability department through daily consultation of the UNSC's official website.

6. MAINTENANCE OF ANALYSIS DOCUMENTS

The files and documents related to the analysis of transactions or selected proposals, whether or not they result in reports to COAF, shall be retained for a period of ten (10) years, in accordance with current regulations.

7. COMPLIANCE, AML/CFT, AND SOCIAL, ENVIRONMENTAL, AND CLIMATE RISK COMMITTEE

Banco Fibra has established the Compliance, AML/CFT, and Social, Environmental, and Climate Risk Committee. Among the topics addressed in this forum are the approval and discussion of highly relevant matters involving Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction. The responsibilities of this committee also include monitoring the Integrity Program, ensuring the dissemination of integrity standards and ethical conduct as part of the institution's culture, among other duties, as detailed in 01-07-19/1 NI Committee Organization.

All decisions must be formalized in meeting minutes and retained for a period of ten (10) years.