ANTI-MONEY LAUNDERING (AML), COUNTER-TERRORIST FINANCING (CTF), AND COUNTER-PROLIFERATION FINANCING POLICY – AML/CTF/CPF

Version 21 – Jan/26

1. Definition

This policy sets out, for employees, partners, suppliers and third-party service providers, the guidelines and best practices for preventing and combating money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction ("ML/CTF/CPF") at Banco Fibra S.A. and its subsidiaries, reinforcing the Bank's commitment to clients and to society, in line with the applicable regulatory framework.

This policy is based on Banco Fibra's Internal Risk Assessment ("IRA") and establishes criteria and procedures that are consistent with the risk profiles of clients, the institution, operations, transactions, products and services, as well as of employees, partners, suppliers and outsourced service providers.

2. Scope

Banco Fibra, its subsidiaries, and its Cayman Branch (hereinafter jointly referred to as "Banco Fibra" or the "Bank").

3. Description

Money Laundering

Money laundering is the act of concealing the illicit origin of assets, funds or values in order to reinsert them into the formal economy under the appearance of legitimacy. In line with international best practices, Brazilian law provides penalties for those who conceal or disguise the nature, origin, location, disposition, movement or ownership of assets, rights or values derived, directly or indirectly, from a criminal offense. The same penalties apply to anyone who, with the purpose of concealing or disguising the use of assets, rights or values originating from a criminal offense, engages in: (i) conversion into lawful assets; (ii) obtaining, receiving, exchanging, negotiating, providing or receiving as collateral, safekeeping, deposit, movement or transfer; (iii) importing or exporting goods at values that do not reflect their true worth; (iv) using, in economic or financial activity, assets, rights or values originating from a criminal offense; and (v) participating in a group, association or office, knowing that its main or secondary activity is directed at crimes provided for in applicable laws.

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

Terrorism consists in the practice, by one or more individuals, of the acts described below, for reasons of xenophobia, discrimination or prejudice based on race, color, ethnicity or religion, when committed with the purpose of causing social or generalized terror, endangering people,

property, public peace or public safety. Acts of terrorism include: (i) using or threatening to use, transporting, keeping, carrying or possessing explosives, toxic gases, poisons, biological, chemical or nuclear agents, or other means capable of causing damage or mass destruction; (ii) sabotaging or seizing, with violence, serious threat, or through cyber means, total or partial control, even temporarily, of means of communication or transport, ports, airports, railway or bus stations, hospitals, clinics, schools, stadiums, public facilities or locations that provide essential public services, power generation or transmission facilities, military facilities, oil and gas exploration, refining and processing facilities, and banking institutions and their service networks; and (iii) attempting against a person's life or physical integrity.

Additionally, as defined by United Nations Security Council (UNSC) resolutions, States are required to halt any support to non-state actors for the development, acquisition, production, possession, transport, transfer or use of nuclear, biological and chemical weapons and their delivery systems. Governments, through their institutions, must adopt measures to identify and mitigate the risks of proliferation financing, in addition to money laundering and terrorist financing.

Scope and Application of Sanctions

Brazilian law provides stringent penalties for anyone who offers or receives, obtains, keeps, deposits, requests, invests, or otherwise contributes to obtaining any asset, good or financial resource to finance, in whole or in part, a person, group of people, association, entity or criminal organization whose principal or secondary activity, even if occasional, is the practice of the crimes described above.

Banks and other financial agents, their representatives and employees, must implement mechanisms to prevent money laundering, terrorist financing and proliferation financing, making it difficult or impossible, and/or reporting the occurrence or suspicion of illicit activity. Banco Fibra's employees, subsidiaries, partners, suppliers and outsourced service providers who are negligent, omissive or complicit are subject to administrative and civil sanctions, regardless of their role at the Bank. It is the responsibility of Management and of each employee, partner and third-party service provider to comply with ML/CTF/CPF laws and regulations and to immediately notify the Compliance & Sustainability area of any breach of this policy or of any suspicious operations at compliance.pld@bancofibra.com.br.

3.1 Institutional Guidelines

Prevent ML/CTF/CPF in Banco Fibra's business in Brazil and abroad, in line with Brazilian law and with the laws of the countries where it operates;

Strictly comply with the AML/CTF/CPF policy, including procedures, controls and the timely correction of identified deficiencies;

Perform duties and manage relationships with clients, employees, partners, suppliers and outsourced service providers in accordance with the Integrity Program's anti-corruption and anti-fraud procedures (Law No. 12,846/13 – Brazilian Anti-Corruption Law);

Act consistently with Brazil's international commitments to prevent and combat ML/CTF/CPF;

Engage in joint actions in the national and international financial system to prevent and combat ML/CTF/CPF and corruption;

Identify, qualify and classify clients and keep their records up to date;

Do not initiate relationships before completing client identification, qualification and classification;

Maintain internal controls and consolidated records to verify client identification/qualification/classification and the compatibility between resource movements, economic activity and financial capacity;

Do not allow transactions through anonymous or fictitious accounts;

Keep records of all operations involving domestic/foreign currency, securities, precious metals or any other asset convertible to cash;

Maintain internal controls to detect transactions that indicate ML/CTF/CPF;

Adopt measures to inhibit ML/CTF/CPF when developing or reviewing products and services, including when adopting new technologies;

Every two years, or when risk profiles change significantly, perform the Internal Risk Assessment (IRA);

Perform the Effectiveness Assessment of AML/CTF/CPF processes, including policy, 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 providers, into risk categories, in line with the IRA;

Use regulatory parameters to record transactions and to identify those indicating ML/CTF/CPF in the design or acquisition of automated monitoring systems;

Carefully analyze instruments, channels, execution method, parties and values, financial capacity, client's business activity, purpose and any indication of irregularity or illegality;

Report to the competent authorities, within legal deadlines and formats, transactions or proposals that indicate ML/CTF/CPF;

Confidentially record, analyze and report to competent authorities any suspicious transactions or those meeting mandatory reporting criteria;

Apply restrictive measures and prevent business with clients, employees, partners, suppliers or outsourced providers when circumstances indicate ML/CTF/CPF or corruption;

Maintain correspondent relationships only with institutions that have adequate AML/CTF/CPF and anti-corruption controls;

Adopt criteria for hiring and conduct of employees (KYE) and of partners/suppliers/outsourcers (KYP);

Maintain specific training programs for relevant employees and third parties.

3.2 AML/CTF/CPF Procedures

Internal Risk Assessment (IRA)

The Compliance & Sustainability area performs the IRA under a Risk-Based Approach (RBA) to identify ML/CTF/CPF risks considering: (i) clients; (ii) the institution and its business model/geographic footprint; (iii) operations, transactions, products and services, including distribution channels and the use of new technologies; and (iv) activities performed by employees, partners, suppliers and outsourced providers. The IRA categorizes risks by probability and by financial, legal, reputational and social/environmental impacts and is reviewed at least every two years or upon material changes.

Clients are classified into the following risk categories: Very Low, Low, Medium, High and Very High, and are subject to identification, qualification and monitoring criteria, with approvals as set forth in NI 01-07-06/1 KYC. Partners (including suppliers and outsourced providers) are classified as High, Medium or Low in accordance with NI 01-07-24/1 KYP. Employees and candidates are classified as High, Medium or Low under NI 01-14-07/1 KYE. Risk classifications may change over time as new facts emerge.

Know Your Customer (KYC)

KYC is required by regulators and establishes adequate rules and procedures to identify and qualify clients and to understand their wealth and the origin of funds. Banco Fibra standardizes procedures for onboarding, maintenance and monitoring of clients who use or intend to use the Bank’s products and services, so as to prevent any collaboration with ML/CTF/CPF or other illicit activities. Procedures aim to ensure, at any time, the client’s identity (who they are), activity (what they do), and consistency in the origin and movement of funds. Enhanced measures apply to higher-risk clients, such as shorter KYC review cycles and inclusion in special monitoring lists.

Client Registry

The client registry is a cornerstone of KYC and is carried out according to the client's relationship profile, in line with regulation. It includes information collected from the client and from public/private databases, document checks and the ongoing update of data in a secure repository. The registry must identify ultimate beneficial owners (UBOs) – the natural persons who ultimately own, control or significantly influence the entity (for legal entities). Additional details are available in NI 01-12-06/1 Client Onboarding & Maintenance and NI 01-07-06/1 KYC.

Client Risk Rating (AML/CTF/CPF)

At onboarding or KYC renewal, all clients are risk-rated based on the KYC form, combining registry data, relationship history, geographic location, PEP identification, reputational checks, restrictive/sanctions list screening and UBO identification percentage, resulting in a rating (Very High, High, Medium, Low or Very Low) in accordance with the IRA. Approvals follow the levels set out in NI KYC.

Foreign Exchange Operations

Banco Fibra applies enhanced due diligence to clients conducting FX transactions to prevent irregularities and crimes related to ML/CTF/CPF, using controls and systems that ensure the regularity, economic and legal purpose of the operation and the client's financial capacity.

Politically Exposed Persons (PEPs)

PEPs are identified through client declarations and independent screening by Compliance & Sustainability using PEP databases. The presence of PEPs in the ownership structure is considered as a risk factor in the AML/CTF/CPF assessment and in the final risk classification. The area performs enhanced monitoring of all PEP clients or transactions involving PEPs/related parties. Companies with partners or officers identified as PEPs are also treated as PEPs (expanded PEP concept). Eligible positions/conditions are detailed in guide 01-07-06/2 KYC.

Monitoring, Selection, Analysis and Reporting (MSAR)

The Bank continuously monitors financial transactions and client operations to identify situations that may indicate ML/CTF/CPF and other occurrences subject to reporting to the Financial Intelligence Unit (COAF), the Prizes and Betting Secretariat (SPA) or the competent authorities in other jurisdictions. Monitoring uses automated rules via a specialized vendor system. Alerts are assessed by Compliance & Sustainability for reporting applicability, except for cases outside mandatory reporting criteria, as per GP 01-07-17/2 AML/CTF.

Monitored information is confidential and access-restricted to Compliance, which defines processes and controls and keeps dossiers for at least the minimum period required by applicable regulation for audit and supervisory review.

Cash Transactions

Although the Bank does not process cash transactions under its business model, such operations are preventively covered by monitoring rules (e.g., cash deposits, increased cash deposit frequency, or volumes above Central Bank thresholds). Receipt of checks must be previously informed by Operations (Agency & Judicial Orders) for Compliance & Sustainability review and, when necessary, escalation to the Compliance, AML/CTF/CPF and Social, Environmental & Climate Risk Committee.

Reporting of Fraud and Suspicious Transactions

All transactions or proposals that may indicate suspicious situations, or that fit mandatory reporting conditions, must be reported to COAF and to competent regulators in relevant jurisdictions. Suspicious ML/CTF/CPF cases are deliberated by Compliance & Sustainability and, when applicable, by the Committee, with decisions recorded in minutes. If reporting is approved, it must occur by the next business day. Employee identity must be preserved; Compliance & Sustainability is responsible for filings; communications are made without notice to involved parties; and clients/prospects must not be informed. Monitoring/selection must occur within 45 days of the event date. COAF scores communications via SISCOAF; Compliance reviews the scores monthly and implements improvements as needed. If no communications were made during the year, Compliance must submit a 'no-filings' notice within the first ten business days of January, including for subsidiaries when applicable.

Reporting of Irregular Betting Accounts (SPA)

Cases of suspected irregular betting accounts must be reported to the Secretaria de Premios e Apostas (SPA) within 24 hours of identification, via the SEI (Electronic Information System), with a report including: reasons supporting the suspicion; the CNPJ of the legal entity involved; and its corporate name.

Know Your Partner (KYP)

KYP applies to partners, suppliers and outsourced providers (relevant or not) and must be performed before onboarding or upon renewal, via the Know Your Partner form (Supplier, Relevant Supplier, Brokers and other categories per NI 01-07-24/1 KYP). It covers AML/CTF/CPF and anti-corruption aspects before onboarding and during periodic renewals, with the objective of avoiding relationships with counterparties involved or suspected of illicit activities (e.g., corruption, ML/CTF/CPF, environmental, social or climate-related harm) and ensuring that such counterparties have adequate AML/CTF/CPF procedures when applicable. Risk assessment performed by Compliance & Sustainability classifies partners as High, Medium or Low based on the Third-Party Due Diligence Questionnaire and supporting compliance research. Site visits may be conducted with the support of Procurement or the Commercial area as applicable. All parties may report concerns to the Ethics Hotline, per NI 01-07-25/1.

Know Your Employee (KYE)

Prior to hiring, the Bank collects and verifies candidate information (conflicts of interest, reputation, registry, etc.). Upon hiring, each employee must sign a Conflict of Interest Statement and update it upon any new fact, as detailed in NI KYE. Compliance & Sustainability assesses ML/CTF/CPF risk of candidates (employees and interns) under the IRA and classifies them as High, Medium or Low. The active employee base is reviewed annually to identify changes in risk level. Managers must promptly inform Compliance & Sustainability (compliance.pld@bancofibra.com.br) of relevant changes in an employee's socio-economic profile, repeated non-compliance with AML/CTF/CPF rules, or behavioral changes that may pose risk. Employees may also report concerns to the Ethics Hotline (NI 01-07-25/1).

Assessment of New Products and Services

New products and services are subject to prior AML/CTF/CPF review by Compliance & Sustainability, per the Product & Service Development policy, with outcomes recorded in the Product Approval Form (FAP). New technologies are also subject to prior AML/CTF/CPF risk assessment, including the evaluation of service providers when applicable.

Effectiveness Assessment

The Internal Controls & Operational Risk area annually assesses the effectiveness of this policy, procedures and controls. The assessment covers: (i) KYC (including registry); (ii) monitoring, selection, analysis and reporting to COAF (including parameter effectiveness); (iii) AML/CTF/CPF governance; (iv) organizational culture measures; (v) periodic training programs; (vi) procedures to know employees/partners/suppliers/outsourcers; and (vii) remediation of audit and supervisory findings. The annual report must be sent to the Audit Committee (COAUD) and the Board of Directors (BoD) by March 30 each year. Action plans are tracked by Internal Controls and formalized in a Follow-up Report by June 30 each year for review by Management, COAUD and the BoD.

Systems for AML/CTF/CPF

The Bank uses market solutions to perform necessary AML/CTF/CPF controls and procedures, including background checks, sanctions/restrictive list screening, PEP screening, negative media and other checks related to financial crime, ML/CTF/CPF, and social, environmental and climate risks. KYC analyses and risk ratings are recorded in a dedicated system.

Other AML/CTF/CPF Procedures

The Bank performs due diligence on counterparties not covered by KYC/KYE/KYP (e.g., potential buyers of assets from BNDU sales, assignment of restructured credit operations), and only executes transactions with reputable parties. Suspected cases must be reported to COAF or other applicable authorities.

3.3 Training

The dissemination of ML/CTF/CPF concepts and the commitment of Senior Management and all employees are fundamental to the effectiveness of prevention and combat actions. Banco Fibra maintains a training and awareness program on ML/CTF/CPF for all employees. Trainings ensure employees can identify situations that may indicate ML/CTF/CPF and report them to the area responsible for assessment and regulatory reporting. Trainings are delivered at least annually and are mandatory for all new hires. The People & Culture area issues electronic reminders to employees with pending trainings and reports non-completion to Compliance & Sustainability.

3.4. Assignment of Responsibilities

• Board of Directors

- Approve the annual review of this policy; and
- Receive and approve the annual report resulting from the effectiveness tests, as well as monitor the implementation of action plans proposed to address the identified risks.

• AML/CTF/CPF Director

- Promote the AML/CTF/CPF culture among employees, partners, suppliers, and outsourced service providers, as applicable, including the adoption of periodic training programs;
- Monitor compliance with the AML/CTF/CPF policy, rules, procedures, and controls, as well as their updates, to ensure the proper management of risks related to the topic;
- Enforce disciplinary actions against employees, partners, suppliers, and outsourced service providers who fail to comply with AML/CTF/CPF procedures;
- Oversee the activities of the AML/CTF/CPF area, as well as the Compliance, AML/CTF/CPF 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 data necessary to perform their duties and those of their team, especially regarding the effective management of AML/CTF/CPF risks;
- Allocate adequate resources for the maintenance and enhancement of the AML/CTF/CPF program; and
- Ensure that the AML/CTF/CPF program is reviewed regularly to guarantee its efficiency and effectiveness, incorporating new risk factors when applicable.

• Compliance, AML/CTF/CPF and Social, Environmental and Climate Risk Committee

- Monitor the Integrity Program, ensuring the dissemination of integrity and ethical conduct standards 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 continued effectiveness and application of the procedures, principles, and guidelines established therein;
- Recommend corrective measures whenever non-compliance with the procedures and guidelines of the Compliance Policy is identified;
- Assess cases involving clients, partners, suppliers, or outsourced service providers, analyzed by AML/CTF/CPF Compliance, where indicators of crime or irregularities require higher-level decision-making; and
- Evaluate cases involving clients, partners, or outsourced service providers analyzed by Compliance related to Social, Environmental, and Climate Risks requiring higher-level decisions.

• Compliance & Sustainability Department

- Promote the implementation, maintenance, and update of governance, rules, and procedures related to the Bank's AML/CTF/CPF program, including Know Your Customer (KYC), Know Your Employee (KYE), Know Your Partner (KYP), and Monitoring, Selection, Analysis and Reporting of suspicious activities;
- Ensure, together with Senior Management, the existence, update, and enforcement of AML/CTF/CPF policies, guidelines, and internal control procedures;
- Monitor the adequacy of the AML/CTF/CPF program;
- Act independently and autonomously to avoid conflicts of interest;
- Ensure the prevention, detection, and reporting of transactions that may indicate crimes defined in applicable legislation;
- Have full access to all information deemed necessary to perform AML/CTF/CPF risk governance;
- Promote the AML/CTF/CPF culture among employees and service providers by adopting periodic training and communication initiatives related to AML/CTF/CPF and anti-

corruption, with the purpose of fostering and maintaining a culture of integrity within the organization;

- Interact with regulatory and self-regulatory agencies on AML/CTF/CPF matters;
- Immediately comply, without prior notice to sanctioned individuals or entities, with United Nations Security Council (UNSC) sanction resolutions or committee designations mandating asset freezes;
- Apply procedures to address identified breaches and deficiencies in the AML/CTF/CPF program and notify Senior Management based on the assigned risk level, through operational risk event reporting as defined in internal policies;
- Recommend to the Compliance, AML/CTF/CPF and Social, Environmental, and Climate Risk Committee the termination of client relationships whenever AML, terrorism financing, or reputational risk is identified; and
- Maintain confidentiality over data and information related to indications of money laundering, asset concealment, or terrorism financing, which must not be recorded in databases of fraud attempts or suspicious activity indicators, as required by applicable regulations.

• Internal Controls Department

- Perform annual effectiveness tests of the AML/CTF/CPF policy, procedures, and internal controls;
- Monitor and provide adequate governance over action plans arising from the effectiveness tests; and
- Record operational risk events related to AML/CTF/CPF and follow up on corrective action plans until fully implemented.

• Commercial Department

- Ensure relationships are established only with reputable clients, applying best efforts to properly conduct onboarding and KYC procedures; and
- Immediately notify the Compliance & Sustainability area whenever suspect behavior by clients indicates possible AML/CTF/CPF activity or conflicts with the Bank’s Integrity Program.

• All Employees

- Comply with AML/CTF/CPF policies, rules, procedures, and internal controls, accessing internal standards and process guides whenever needed, and completing periodic training available on the Bank's Intranet; and
- Report promptly any indication of unusual AML/CTF/CPF activity, corruption, or fraud to the Compliance & Sustainability area or through the Ethics Hotline.

• Partners, Suppliers, and Outsourced Service Providers

- Comply with all applicable guidelines described in this policy; and
- Report promptly any indication of unusual AML/CTF/CPF activity, corruption, or fraud to the Ethics Hotline related to Banco Fibra's activities.

3.5. Information Maintenance

Client registry records shall be stored physically or electronically, based on the documents required in the Onboarding and Registry Maintenance NI, in a dedicated and protected archive. Records for employees, partners, suppliers, and outsourced service providers shall be stored according to the procedures established in the KYE and KYP guidelines.

Adherence to the principles of KYC, KYP, and KYE, as well as document requests, must be proportional to the risk profile of each client, provider, or employee, as applicable.

3.6. Other Provisions

The guidelines set forth in this policy also apply to services provided by Banco Fibra in the capacity of distributor or custodian.

---

4. Compliance Deliberation

The Compliance Deliberation process applies to cases requiring higher-level decisions that do not need to be reviewed by the Compliance, AML/CTF/CPF and Social, Environmental and Climate Risk Committee. The responsibility for analysis and deliberation lies with the Compliance Management, together with the AML/CTF/CPF Director.

Applicable assessments include:

- Reporting to COAF cases defined by applicable legislation;
- Other compliance matters not requiring Committee review; and
- Matters related to Social, Environmental, and Climate Risk.

All decisions made by the area and/or the Committee must be documented in meeting minutes and stored for ten (10) years.

---

5. Asset Freezing

The Compliance & Sustainability area is responsible for monitoring UNSC (United Nations Security Council) asset-freezing determinations, both during client onboarding/KYC and throughout ongoing monitoring of financial transactions during the client relationship.

Daily screening is conducted through market systems covering all active clients against sanctions lists containing individuals, legal entities, and organizations designated under UNSC resolutions. Lists are updated by the vendor, and Compliance & Sustainability periodically verifies the integrity of list information.

If a client is identified as a match, Compliance & Sustainability must notify the Operations and Credit Monitoring areas, which will immediately freeze assets through the Dashboard system under the status “UNSC Block.”

Compliance & Sustainability must also immediately notify:

- The Central Bank of Brazil (via BC Correio);
- COAF- Conselho de Controle de Atividades Financeiras (via its reporting system); and
- The Ministry of Justice and Public Security (MJSP) through csnu@mj.gov.br.

Any additional information required to comply with UNSC measures is monitored daily through the UNSC website.

---

6. Retention of Analysis Documentation

Dossiers and documents related to analyzed operations or proposals—whether reported to COAF or not—must be stored for ten (10) years, as required by applicable regulation.

---

7. Compliance, AML/CTF/CPF and Social, Environmental and Climate Risk Committee

Banco Fibra maintains a Compliance, AML/CTF/CPF and Social, Environmental and Climate Risk Committee. This forum discusses and approves highly relevant matters involving money laundering, terrorist financing, and the proliferation of weapons of mass destruction.

The Committee is also responsible for monitoring the Integrity Program and promoting integrity and ethical conduct as part of the Bank's culture, in accordance with NI 01-07-19/1 Organization of Committees.

All decisions are documented in meeting minutes and retained for ten (10) years.