

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

AML Policy

Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda.

Contents

1. Purpose	2
2. Scope	2
3. Terms and Definitions	4
4. General Guidelines	5
4.1 Preventive actions	5
4.2 Virtual assets and stablecoins	5
a) Monitoring of virtual asset transactions	6
b) Regulatory coverage	6
c) Integration with KYC procedures	6
4.3 Know your client, supplier and employee	6
4.3.1 General guidelines for the know-your processes	6
4.3.2 Know Your Customer (KYC/KYB)	7
4.3.3 Know Your Employee (KYE)	8
4.3.4 Know Your Partner and Supplier (KYP/KYS)	9
4.3.5 Know Your Product and Service	10
4.4 Handling of occurrences and reporting	10
4.4.1 Monitoring and selection of atypical transactions and situations	10
4.4.2 Analysis of selected transactions and situations	11
4.4.3 Reporting to Coaf and decision on the relationship	11
4.4.4 Information security and cyber incidents	12
4.4.5 Other occurrences and non-conformities	12
4.4.6 Recording and traceability	13
4.4.7 Whistleblowing channel	13
4.5 Training	13
4.6 Independent review	13
5. Records	14

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

6. Review	15
7. Reference Standards	15
8. Effectiveness	16
9. Version Control and History	17

1. Purpose

This Policy sets out the rules and procedures to be observed by Trace Finance with regard to the conduct of all employees within the program for the prevention of and fight against money laundering and the concealment of assets, rights and values, and for the prevention of terrorist financing, in accordance with the applicable regulations.

The main objectives of this Policy are to:

- Establish guidance, definitions and procedures to prevent and detect operations or transactions with atypical characteristics, in order to combat the crimes of money laundering or concealment of assets, rights and values, as well as to identify and monitor transactions carried out with politically exposed persons, always with a view to the integrity of Trace Finance, the foreign exchange market and global banking;
- Determine the organizational structure, reinforcing Trace Finance's commitment to comply with anti-money laundering and counter-terrorist financing laws, in addition to identifying products, services and areas that may be vulnerable to such practices;
- Emphasize the importance of knowing clients, employees and third parties, as well as of reporting suspicious activities;
- Define the employee training program.

Trace Finance seeks to cooperate fully with government bodies in detecting, preventing and combating the activities addressed herein, so as not to be used inadvertently as an intermediary in a process aimed at money laundering or terrorist financing. The aim is thereby to maintain the integrity and proper functioning of the market, with client protection, transparency, prevention of conflicts of interest and information symmetry.

2. Scope

This Policy applies to all employees, officers, interns, apprentices and service providers of Trace Finance, as well as to third parties, partners and suppliers acting for or on behalf of the organization, and to all products, services, transactions and relationships maintained by it.

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

All employees are responsible for knowing and complying with the obligations arising from this Policy and from the legislation in force, as well as for observing the highest standards of professional conduct in carrying out their activities. Everyone also has the duty to inform and report inconsistencies in the procedures and practices defined in this document to their immediate superior and to the Compliance department.

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

3. Terms and Definitions

Term	Definition
Money Laundering	Process by which funds originating from illegal activities are transformed into assets of apparently legal origin. The practice generally involves multiple transactions used to conceal the origin of the funds and allow them to be used in a way that makes them appear lawful. It consists of three stages: (i) placement: introduction into the financial system of funds from illicit activities, through deposits or the purchase of financial instruments or goods; (ii) layering: execution of multiple financial transactions with the funds already introduced, through complex and numerous transactions, to hinder the tracing and identification of the illegal source; and (iii) integration: formal incorporation of the money into the economic system, through investment in the capital markets, real estate, works of art, among others.
Terrorist Financing	Process of concealed distribution of funds to be used in terrorist activities. Such funds generally originate from the activities of other criminal organizations involved in drug, arms and ammunition trafficking and smuggling, or may derive from illicit activities, including donations to sham charities. The methods used to conceal the link between the agents and the sources of financing are similar to those used in money laundering, although the use of legally obtained funds is common, in order to reduce the risk of discovery before the terrorist act.
PEP (Politically Exposed Person)	Public official who holds or has held, in the last five years, relevant public positions, employment or functions, in Brazil or abroad, as well as their representatives, family members and close associates, in accordance with the applicable regulation.
Ultimate Beneficial Owner	Natural person who ultimately owns, controls or significantly benefits from the corporate client, supplier or partner.
KYC, KYE and KYP/KYS	Structured processes for knowing and verifying clients (Know Your Customer), employees (Know Your Employee) and partners and suppliers (Know Your Partner / Know Your Supplier), governed by the subordinate instruments indicated in Section 4.3.
AIR (Internal Risk Assessment)	Documented and periodic assessment of the risks of the organization being used for money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction, approved by the Officer responsible for AML.
Virtual Asset	Digital representation of value traded or transferred by electronic means and used to make payments or for investment purposes, including stablecoins.

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

Term	Definition
Travel Rule	Rule for the identification and transmission of originator and beneficiary data in transfers of funds and virtual assets above the defined thresholds.

Note: the Brazilian regulatory framework of this Policy is in line with international legislation, Brazil being a signatory to the main international commitments related to the subject.

4. General Guidelines

4.1 Preventive actions

The measures adopted to combat and prevent the flow of potential illicit transactions by third parties through Trace Finance include:

- Know Your Customer, Know Your Employee and Know Your Partner and Supplier procedures, referred to in Section 4.3;
- Investment in internal training;
- Investment in appropriate tools for the diligent performance of duties.

Trace Finance adopts measures to prevent or mitigate money laundering and terrorist financing proportionally to the risks identified in the process of accepting and maintaining the relationship with the end client, within the limits of its duties. Third parties are classified according to Low, Medium or High risk levels, considering: the sensitivity of the information accessed; the potential impact on the business; the degree of operational dependence; the associated regulatory requirements; and the level of access granted to systems and data.

Trace Finance does not tolerate dealings of any kind with countries subject to economic sanctions or designated as state sponsors of terrorism, such as those on the UN list or the list of the Office of Foreign Assets Control (OFAC), or with companies with bearer shares.

4.2 Virtual assets and stablecoins

Trace Finance carries out purchase and sale transactions of virtual assets, including stablecoins, on behalf of exchanges and institutional counterparties. These transactions are subject to the same anti-money laundering and counter-terrorist financing controls applicable to the organization's other transactions, observing the following guidelines:

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

a) Monitoring of virtual asset transactions

All orders involving virtual assets, including stablecoins, are subject to automated screening through a specific tool that traces the origin and destination of the assets and identifies exposure to sanctioned addresses, mixers or high-risk entities. Transactions that exceed the configured risk parameters are forwarded to the Compliance team for manual approval.

b) Regulatory coverage

Virtual asset transactions are aligned with BCB Resolutions No. 519, 520 and 521/2025, applicable to Virtual Asset Service Providers (PSAV), and with the FATF recommendations for VASPs, in particular with regard to transaction monitoring and the Travel Rule for transactions above USD 1,000.

c) Integration with KYC procedures

The onboarding process for counterparties that transact in virtual assets follows the due diligence criteria defined in this Policy and detailed in the KYC procedure, applied proportionally to the identified risk profile.

4.3 Know your client, supplier and employee

As an integral part of the anti-money laundering and counter-terrorist financing program, Trace Finance adopts structured procedures for knowing and verifying all its relationships: clients, employees, and partners and suppliers. These procedures are applied proportionally to the level of risk identified in each relationship and constitute an essential measure for Trace Finance's operational integrity.

4.3.1 General guidelines for the know-your processes

a. Risk-based approach: the depth of due diligence is proportional to the risk identified in the client, the product and the jurisdiction, with enhanced measures for higher-risk categories, as set out in the Internal Risk Assessment (BCB Circular No. 3,978/2020, articles 13, paragraph 1, I, and 20);

b. Mandatory consistency: the know-your procedures must be consistent with this Policy and with the Internal Risk Assessment, an express requirement both for clients (article 13, paragraph 1, II and III) and for employees, partners and outsourced service providers (article 56, sole paragraph);

c. Due diligence prior to the relationship: it is prohibited to begin a business relationship before the client identification and qualification procedures have been completed (article 23);

d. Formalization in a specific procedure: the know-your-client processes are formalized in a specific procedure, approved by the institution's board and kept up to date (article 13,

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

paragraphs 2 and 3). The criteria for defining the necessary information and the verification, validation and updating procedures for each risk category are set out in that procedure (article 22);

e. Single chain of responsibility: all subordinate instruments indicate the same Officer responsible for AML formally appointed to the Central Bank of Brazil (article 9);

f. Single program assessment: a single Internal Risk Assessment (article 10) and a single annual effectiveness assessment report (article 62) cover all know-your processes, partial assessments per instrument being prohibited;

g. Organizational culture of prevention: awareness actions reach not only employees but also partners and outsourced service providers (article 3, I, "e");

h. Traceability: the checks carried out allow their reconstruction and audit, with a record of the source consulted, the date and the person responsible;

i. Confidentiality and data protection: the information obtained is treated confidentially and accessed only by authorized persons, observing the principles of need-to-know and least privilege and the requirements of the LGPD.

4.3.2 Know Your Customer (KYC/KYB)

The guidelines of the know-your-customer process are:

a. Identification: adopt procedures to verify and validate the client's identity, including by cross-checking against public and private databases, collecting at a minimum the full name and CPF, in the case of natural persons, or the corporate name and CNPJ, in the case of legal entities, with specific treatment for persons resident or domiciled abroad who are exempt from registration (article 16);

b. Qualification: collect, verify and validate information that makes it possible to identify the place of residence, head office or branch and to assess the client's financial capacity, including income or revenue, as well as additional information consistent with the risk of use of the products and services. Qualification is permanently reassessed and the information kept up to date (article 18);

c. Classification: classify the client into the risk categories defined in the Internal Risk Assessment, based on the information obtained in the qualification, reviewing the classification whenever there is a change in the risk profile or in the nature of the business relationship (article 20);

d. Extension to officers and representatives: apply the identification, qualification and classification procedures to officers of corporate clients and to client representatives, in a manner consistent with the function performed and the scope of the representation (article 21);

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

e. Ultimate beneficial owner: identify the natural person who ultimately owns or controls the corporate client, by analyzing the chain of ownership, adopting an ownership threshold of no more than 25%, the start of the business relationship being prohibited without the conclusion of this identification (articles 24 and 25);

f. Politically exposed person: adopt procedures to qualify the client as a PEP, as well as their family members and close associates, with enhanced due diligence and approval at a higher hierarchical level, the status being maintained for five years after the date on which the person ceased to qualify (articles 19 and 27, paragraph 5);

g. Graduated due diligence: apply simplified, standard or enhanced due diligence in proportion to the risk category, classification as low risk being prohibited in the presence of a binding prohibition factor or of mandatory classification as high risk;

h. Refusal and termination: refuse to open a relationship or terminate an existing relationship when it is not possible to form a reasonable conviction as to the client's true identity, or in the event of false or incomplete information or unjustified refusal to complete the process;

i. Periodic update of records: reassess the client record and rerun sanctions and PEP checks at a frequency defined by risk category.

4.3.3 Know Your Employee (KYE)

The guidelines of the know-your-employee process are:

a. Identification and qualification: implement procedures to know employees, including identification and qualification, consistent with this Policy and with the Internal Risk Assessment (article 56 and sole paragraph);

b. Selection and hiring: take into account, in the selection and hiring of employees and outsourced service providers, the risk of money laundering and terrorist financing (article 3, I, "f");

c. Training: subject employees to a training program on the prevention of money laundering and terrorist financing (article 3, I, "g");

d. Conflict of interest: assess conflicts of interest and connections that may represent a risk to the organization, with a formal declaration and reassessment upon events;

e. Legal limits of checks: conduct background checks within the limits of labor legislation and the LGPD, with a specific purpose, documented justification and proportionate retention;

f. Maintenance throughout the relationship: maintain the process throughout the employment relationship, with an annual periodic review and an extraordinary review upon

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

an indication of irregularity, an information security incident, a whistleblowing report or an internal investigation.

4.3.4 Know Your Partner and Supplier (KYP/KYS)

The guidelines of the know-your-partner-and-supplier process are:

a. Identification and qualification: implement procedures to know partners and outsourced service providers, consistent with this Policy and with the Internal Risk Assessment (article 56 and sole paragraph), observing the measures for knowing business partners and outsourced service providers required by BCB Resolution No. 520/2025, article 47;

b. Due diligence prior to contracting: make contracting conditional on the completion of due diligence proportional to the third party's risk classification, with a record of the risks identified, the treatment measures and the decision, except for the waiver cases provided for in the specific procedure, approved at the authority level defined therein and formally recorded;

c. Third-party risk classification: classify third parties into risk categories considering the criticality of the services, the sensitivity of the information accessed, the level of access granted, operational dependence, the associated regulatory requirements and the AML nature of the supplier's activity;

d. Sanctions and PEP screening: subject the partners, officers and ultimate beneficial owners of third parties classified as critical or high risk, whose activity relates to virtual assets, foreign exchange, custody of funds, correspondent banking or client flows, to screening against sanctions lists and PEP databases, using the same methodology applied to clients;

e. Intragroup relationships: subject relationships with companies of the same economic group to enhanced risk treatment, given the impossibility of a self-referenced assessment, requiring a formalized contract, independent due diligence on the counterparty, segregation of duties and flows, and independent reconciliation;

f. Monitoring and termination: monitor the third party throughout the relationship, proportionally to its criticality, and ensure controlled termination, with revocation of access and return or secure disposal of information;

g. Objective due diligence triggers: require, regardless of the risk classification, a background check and the completion of the partner knowledge form in the cases of value and technical integration with the organization's systems defined in the specific procedure;

h. Waivers: allow the total or partial waiver of the know-your-partner-and-supplier requirements only on an exceptional basis, upon formal justification, for a fixed period and

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

with approval at the authority level, scaled by value and criticality, defined in the specific procedure, the waiver of sanctions and PEP screening and of the enhanced treatment applicable to intragroup relationships being prohibited, with the waivers granted reported to the Compliance Committee.

4.3.5 Know Your Product and Service

Trace Finance maintains procedures for the prior assessment and analysis of new products and services, as well as of the use of new technologies, in view of the risk of money laundering and terrorist financing (article 3, I, "b"). The guidelines of this process are:

- a.** Prior opinion of the Compliance area as a condition for launching a new product or service, or for adopting a relevant new technology;
- b.** Assessment of the exposure of the product or service to money laundering and terrorist financing typologies, and definition of the applicable mitigating controls;
- c.** Reflection in the Internal Risk Assessment and, where applicable, in the risk classification of the clients who contract the product;
- d.** Reassessment whenever there is a relevant change in the characteristics of the product, the distribution channel or the target audience.

4.4 Handling of occurrences and reporting

Occurrences identified by Trace Finance receive segregated treatment according to their nature, as they have different regulatory grounds, approval authorities, deadlines and recipients: atypical transactions and situations subject to the anti-money laundering and counter-terrorist financing regime follow the flow of Sections 4.4.1 to 4.4.3; information security and cyber incidents follow the flow of Section 4.4.4; and other occurrences and non-conformities follow Section 4.4.5. An occurrence of more than one nature is handled cumulatively in each applicable flow, and one flow may not replace another.

4.4.1 Monitoring and selection of atypical transactions and situations

Trace Finance maintains monitoring and selection procedures to identify transactions and situations that may constitute an indication of money laundering, terrorist financing or the financing of the proliferation of weapons of mass destruction. Monitoring is continuous and takes into account the parameters defined in the Internal Risk Assessment, the nature of the products and services provided and the list of transactions and situations in BCB Circular Letter No. 4,001/2020, covering, among other cases, transactions incompatible with the qualification and financial capacity of the person involved, those with a structure or purpose lacking apparent economic grounds, those involving a politically exposed person and those involving a person, entity or jurisdiction subject to sanctions or classified as high risk.

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

The deadline for performing the monitoring and selection procedures does not exceed 45 (forty-five) days from the date of the transaction or situation (BCB Circular No. 3,978/2020, article 39). The selection is recorded with the identification of the person responsible, the date and the parameter, alert or fact that gave rise to it.

4.4.2 Analysis of selected transactions and situations

Selected transactions and situations are analyzed by the Compliance area in order to verify the existence of an indication of money laundering or terrorist financing and to conclude on the need to report to the competent authorities. The deadline for performing the analysis procedures does not exceed 45 (forty-five) days from the date of selection (BCB Circular No. 3,978/2020, article 43).

The analysis is detailed and considers, at a minimum: (i) the record of the client, employee or third party involved, their qualification, financial capacity and risk classification; (ii) the transaction history and transactional behavior, compared with the declared profile and the purpose of the relationship; (iii) the origin and destination of the funds and, in virtual asset transactions, the traceability of the addresses and counterparties involved; (iv) any connection with a politically exposed person, a sanctioned person or entity or a high-risk jurisdiction; (v) the information and clarifications provided by the person involved, when requested; and (vi) the fit of the situation with the applicable typologies and red flags.

The analysis is formalized in a case file, which records the information considered, the checks performed, the grounds and the decision taken, even if the conclusion is not to report, and is kept at the disposal of the Central Bank of Brazil for the period indicated in Section 5. The decision is reasoned and taken by the end of the analysis period (BCB Circular No. 3,978/2020, article 48). It is prohibited to engage third parties to perform the analysis or to carry it out outside Brazilian territory, and the necessary resources and skills must be maintained in Brazil (articles 44 and 45).

4.4.3 Reporting to Coaf and decision on the relationship

Where the analysis concludes that there is an indication, the report to Coaf is made by the business day following the decision to report (BCB Circular No. 3,978/2020, article 48, paragraph 2), indicating, where applicable, politically exposed person status and suspected terrorist financing (article 53); where applicable to Trace Finance's activity, the reports are made by the business day following the date of the transaction, regardless of prior analysis (article 49).

It is prohibited to inform the client, employee, third party involved or any other person of the existence of the report, its analysis or its content (BCB Circular No. 3,978/2020, article 50). Any amendment or cancellation of a report already made, after the fifth business day following its

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

submission, requires the corresponding justification to be recorded (article 51).

Where necessary, the Compliance area decides on the start, suspension or continuation of the transaction and of the relationship with the person involved, whether client, employee or supplier, with the decision and its grounds recorded. When the situation involves a person or entity subject to United Nations Security Council sanctions, asset freezing and the required communications are carried out immediately, in accordance with Law No. 13,810/2019, without prejudice to the flow of this Section.

4.4.4 Information security and cyber incidents

Information security and cyber incidents follow their own flow, which neither replaces nor is confused with the handling of AML occurrences. The incident, including when it involves a third party, is reported to the Information Security and Compliance areas within 24 (twenty-four) hours of its identification and is handled in accordance with Trace Finance's cybersecurity policy, which defines the classification, response, activation of the continuity plan and the required external communications.

Communications to authorities, data subjects and other affected parties observe the deadlines and form defined in the applicable cybersecurity regulation and in Law No. 13,709/2018, which are distinct from the deadlines for reporting to Coaf addressed in Section 4.4.3.

When the incident indicates money laundering or terrorist financing, such as the misuse of credentials or accounts to carry out transactions, the compromise of registration data or the unauthorized movement of funds or virtual assets, the flow of Sections 4.4.1 to 4.4.3 is triggered cumulatively, with the deadlines running from the date on which the indication was identified.

4.4.5 Other occurrences and non-conformities

Occurrences that do not constitute an atypical transaction or situation or an information security incident, such as registration inconsistencies, unjustified refusal to provide information, non-compliance with a requirement of this Policy or non-conformities identified in the due diligence of employees, partners and suppliers, are handled by the Compliance area together with the area responsible for the relationship, with the occurrence recorded, the treatment measure defined and a decision on the continuation of the relationship. An occurrence that, in the course of its handling, reveals an indication of money laundering or terrorist financing is forwarded to the flow of Section 4.4.1.

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

4.4.6 Recording and traceability

Trace Finance must keep a traceable and auditable record of all occurrences handled, including the date of identification, the nature of the occurrence and the applicable flow, the client, employee or third party involved, the measures adopted and the outcome, observing the retention periods of Section 5.

4.4.7 Whistleblowing channel

Situations involving indications of non-compliance with this Policy may be reported, including confidentially and with a prohibition of any retaliation, through the whistleblowing channel maintained by Trace Finance: <https://tracefinance.becompliance.com/canal-etica/canal-denuncias>.

4.5 Training

Trace Finance has an anti-money laundering training program, with the purpose of establishing information channels for team members on the subject and on this Policy.

The training is delivered through an online platform made available to all employees.

Refresher training is launched annually, so that no employee goes more than twelve months without current training.

The training program must be held at least annually and be mandatory for all employees, with completion and results recorded.

4.6 Independent review

The effectiveness of this Policy and of the anti-money laundering and counter-terrorist financing program must be assessed periodically through an independent review, conducted by a person or area not responsible for the execution or direct supervision of the controls assessed, the engagement of a qualified third party being permitted, in accordance with article 12, II, of BCB Circular No. 3,978/2020.

The results of the independent review, including any deficiencies identified and the respective action plans, must be reported to Senior Management and kept as evidence for at least 5 (five) years.

The independent review is distinct from the annual program effectiveness assessment, whose report has a base date of December 31 and is submitted to the Officer responsible for AML and to the Board of Executive Officers by March 31 of the following year (BCB Circular No. 3,978/2020, article 62).

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

5. Records

Documents relating to transactions, including recordings and registration documents, must be retained for a minimum period of 10 (ten) years from the closing of the account or the completion of the last transaction carried out by the client.

Information relating to records of funds transfers must be retained for a minimum period of 10 (ten) years.

Records of the supplier due diligence process, including questionnaires, partner knowledge forms, background check results, acceptance decisions, waiver records and risk treatment plans, must be kept for a minimum period of 10 (ten) years after the end of the relationship.

Without prejudice to the periods indicated above, the table below consolidates the main retention periods applicable to records related to this Policy:

Record category	Retention period	Regulatory basis
Client identification, qualification and ultimate beneficial owner (KYC)	10 years after the end of the relationship	Law No. 9,613/1998; BCB Circular No. 3,978/2020
Case files on the analysis of atypical or suspicious transactions	10 years	BCB Circular No. 3,978/2020, article 67
Records of employees, partners and outsourced service providers	10 years	BCB Circular No. 3,978/2020, articles 56 and 67
This Policy, the AIR and the KYC and monitoring manuals	5 years	BCB Circular No. 3,978/2020, article 66; Law No. 9,613/1998, article 10, III
PEP status, after the person ceases to qualify as such	5 additional years	BCB Circular No. 3,978/2020, article 27, paragraph 5
Results of independent reviews and action plans	5 years	BCB Circular No. 3,978/2020, article 12, II
Records of completion of mandatory training	10 years	BCB Circular No. 3,978/2020, article 67; BCB Resolution No. 520/2025, article 43, paragraph 2

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

6. Review

This Policy must be reviewed periodically or whenever there are relevant changes in Trace Finance's context, in the applicable legal, regulatory or contractual requirements, or as a result of changes in processes, products, services or risks related to the prevention of money laundering and terrorist financing.

Without prejudice to the preceding paragraph, this Policy will be reviewed at least every two years, with approval by the Officer responsible for AML and by Senior Management.

Employees and other applicable parties must always observe the current version of this Policy made available by Trace Finance.

7. Reference Standards

This Policy is aligned with the following laws and regulations:

- Law No. 9,613/1998: Anti-Money Laundering Law, as amended by Law No. 12,683/2012.
- Law No. 13,260/2016: Anti-Terrorism Law.
- Law No. 12,846/2013: Anti-Corruption Law.
- Law No. 13,709/2018: General Personal Data Protection Law (LGPD).
- BCB Circular No. 3,978/2020: provides for the anti-money laundering and counter-terrorist financing policy, procedures and internal controls to be adopted by institutions authorized to operate by the Central Bank of Brazil, including Virtual Asset Service Providers (PSAV).
- BCB Circular Letter No. 4,001/2020: list of transactions and situations that may constitute indications of money laundering or terrorist financing.
- BCB Resolution No. 519/2025: governs the authorization processes related to the operation of virtual asset service provider companies.
- BCB Resolution No. 520/2025: governs the incorporation and operation of virtual asset service provider companies (PSAV).
- BCB Resolution No. 521/2025: governs the activities and transactions of PSAVs in the foreign exchange market.
- Law No. 13,810/2019, BCB Resolution No. 44/2020 and BCB Circular No. 3,942/2019: enforcement of United Nations Security Council (UNSC) sanctions and asset freezing.
- BCB Resolution No. 85/2021: cybersecurity policy and contracting of data processing and storage services.

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

-
- ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection.
 - FATF Recommendations: Financial Action Task Force.

8. Effectiveness

This Policy is permanent in nature. The content of this document may be modified at any time according to current needs. Trace Finance's employees and service providers must, whenever necessary, consult the latest available version.

	AML Policy	CPL-POL-001-FIN
Publication Date: 08/31/2026	Compliance	Public

9. Version Control and History

Version	Date	Change/Addition History	Prepared by	Approved by
1.0	01/2023	Creation of the Policy.	Compliance	Compliance Committee
2.0	07/2024	Policy update: sections 6.3, 8 and 10.	Compliance	Compliance Committee
3.0	03/2025	Policy update: section 6.3.	Compliance	Compliance Committee
4.0	08/2026	Update of scope: the KYC, KYE and KYP/KYS sections now contain the substantive guidelines of the know-your processes, with the step-by-step moved to the specific procedures; inclusion of the sections on Scope, virtual assets and stablecoins, know your product and service, independent review and reference standards. Legislative review: AML regulatory reference (from BCB Res. No. 50/2020 to BCB Circular No. 3,978/2020) and inclusion of BCB Res. No. 519, 520 and 521/2025, Law No. 13,810/2019, BCB Res. No. 44/2020, BCB Circ. No. 3,942/2019 and RFB Normative Instruction No. 2,291/2025; inclusion of the role of Officer responsible for AML. Restructuring and segregation into specific subsections of monitoring and selection, analysis, reporting to Coaf, information security and cyber incidents, other occurrences, recording and the whistleblowing channel, with the deadlines and case file requirement of BCB Circular No. 3,978/2020. Inclusion of the records retention table, with retention extended from 5 (five) to 10 (ten) years, in accordance with article 67. Removal of the Fraud section, which becomes a separate instrument, and of the Relevant Indication section. Definition of a minimum biennial review cycle.	Compliance	Compliance Committee