INSTITUTIONAL POLICY ON ANTI-MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM AND THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (AML-CFTP)		
INFORMATION CLASSIFICATION	**RESPONSIBLE AREA**	**APPLICABLE ENTITIES**
Public	*Compliance*	StoneCo Ltd. and its subsidiaries

APPROVAL	
Approval Date	**Approved by**
12/18/2025	StoneCo Board of Directors StoneCo Executive Board

REVISION HISTORY			
Revision No.	**Description**	**Date**	**Area / Responsible**
01	Policy Creation	09/30/2020	Heloisa Barbosa
02	Policy Update	12/02/2020	Luiza Vaccaro
03	Policy Update	10/08/2021	Luiza Vaccaro
04	Policy Update	12/30/2022	Fabiane Benedetti
05	Policy Update	08/30/2024	Marília Sances / Vitor Diniz
06	Policy Update	11/13/2025	Ana Luiza Drummond

INDEX

1. TERMS AND DEFINITIONS

AML-CFTP: stands for Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation of Weapons of Mass Destruction.

AML-CFTP Deliberative Forum: refers to the body within the AML-CFTP area, composed of the area's Coordination and Management, responsible for deliberating, on a weekly or extraordinary basis, on suspected ML-TFP cases. Its decisions may result in reporting to the FIU, de-accreditation, or continued monitoring.

AML-CFTP Program: refers to the set of processes, procedures, controls, and governance structures implemented to identify and prevent money laundering, terrorism financing, or any criminal activities involving the concealment or misrepresentation of financial resources.

Board of Directors: refers to the governing body responsible for defining the strategic direction and overseeing StoneCo's management.

CBB: stands for the Central Bank of Brazil.

Client: refers to the individual who enters into an agreement to purchase goods or services in exchange for payment.

COAF: stands for the Financial Activities Control Council (Conselho de Controle de Atividades Financeiras), Brazil 's financial intelligence unit established by Law No. 9,613 of March 3, 1998.

Company: refers to StoneCo and its subsidiaries, as applicable.

Effectiveness Assessment: refers to the process used to evaluate the effectiveness of the AML-CFTP policy, as well as its related processes and internal controls.

Employees: refers to any individual working for the Company, including those employed under the CLT (Consolidação das Leis do Trabalho - the Brazilian Labor Code), interns (those with a formal agreement between the Company and an educational institution), and apprentices.

Executive Board: refers to the Directors of StoneCo, elected as "officers" by the Board of Directors, as well as the statutory directors of its subsidiaries, as applicable.

Financing for the Proliferation of Weapons of Mass Destruction: occurs when an individual, directly or indirectly, by any means, provides financial support, supplies, or raises funds with the intent to use them for the proliferation of weapons of mass destruction, which may be biological, chemical, or nuclear.

IRA: stands for "Internal Risk Assessment" for AML-CFTP purposes, a process through which the Company's risks and controls are identified to define its risk appetite. As a result, all processes, policies, procedures, and controls related to AML-CFTP should be aligned with the IRA to ensure that the risks of Money Laundering and Terrorist Financing (ML/TF) are properly addressed.

KYC: acronym for "Know Your Customer", which refers to the process of verifying the identity of Customers and evaluating and classifying their risk profile.

KYE: acronym for "Know Your Employee", which refers to the process of verifying the identity of Employees and evaluating and classifying their risk profile.

KYP: acronym for "Know Your Partner", which refers to the process of verifying the identity of Partners and evaluating and classifying their risk profile.

KYS: acronym for "Know Your Supplier", which refers to the process of verifying the identity of Suppliers and evaluating and classifying their risk profile.

Legal and Compliance Department: refers to StoneCo's department responsible for corporate governance, legal support (including advisory and litigation matters), and the governance, implementation, and monitoring of the AML-CFTP Program, among other duties.

Money Laundering: refers to the criminal practice of concealing or disguising the nature, origin, location, disposition, movement, or ownership of assets, rights, or values derived, directly or indirectly, from a prior crime or offense. These practices typically occur through transactions designed to obscure the illegal origin of funds, followed by the reintegration of these resources into the financial system to disguise their illicit origin.

Orelhão: refers to the Company's whistleblowing channel, which allows for anonymous reporting. It is available to all Employees, Clients, Partners, and Third-Party Service Providers for reporting unethical conduct by any Employee, administrator, Partner, Supplier, or Client that could impact the Company's commercial, ethical or operational interests.

Partners: refers to entities that may play a key role in providing products, services, or essential support to the Company's operations. Partnerships involve the exchange of information, resources, and joint efforts aimed at achieving mutual goals and objectives.

PEP: stands for "Politically Exposed Person" and refers to any public official who currently holds or has held, in the past five (5) years, in Brazil or in a foreign country, territory, or dependency, a prominent public position, job, or function, pursuant to Article 27 of CBB Circular No. 3,978 of January 23, 2020.

Policy: refers to this Institutional Policy on Anti-Money Laundering and Countering the Financing of

Terrorism and the Proliferation of Weapons of Mass Destruction (AML-CFTP).

RBA: stands for "Risk-Based Approach," a methodology used for assessing and managing activities, processes, and systems aiming to better direct efforts and resources in the practice of AML-CFTP based on the likelihood of adverse events occurring and the impact those events may have.

RCA: stands for "Relative or Close Associate", and refers to the representative, family member, or close associate of a Politically Exposed Person. Pursuant to Article 19 of CBB Circular No. 3,978/2020, family members are considered to be relatives in a direct or collateral line up to the second degree, as well as spouses, partners, and/or stepchildren; and a close associate is one who maintains a close relationship with the PEP, such as joint participation in companies or non-incorporated arrangements, acting as an agent, or exercising control over structures created for the benefit of the PEP.

StoneCo: refers to StoneCo Ltd., a company duly incorporated and validly existing under the laws of the Cayman Islands, with its registered office at Harneys Fiduciary (Cayman) Limited, 4th Floor, Harbour Place, 103 Church St., PO Box 10240 KY1-1002, Georgetown, Cayman Islands, registered with under No. 31.752.270/0001-82.

Terrorism Financing: refers to the structuring, custody, administration, or maintenance of financial resources (licit or illicit), moved in a concealed or disguised manner, to finance terrorist activities and/or groups.

Third-Party Service Providers or Third Parties: refers to the entity, its legal representative, and/or agent that provides or is providing outsourced services to the Company.

Ultimate Beneficial Owner: refers to the individual who, ultimately, owns or controls a legal entity, or on whose behalf a transaction is being conducted. It also includes any representative, including an attorney-in-fact or authorized agent, who has effective control over the activities of the client entity.

UNSC: stands for the United Nations Security Council.

2. OBJECTIVE

This Policy aims to consolidate the Company's principles and foundations regarding the prevention of Money Laundering, Terrorism Financing and the Proliferation of Weapons of Mass Destruction, in compliance with applicable laws, regulations, and recognized best practices, both nationally and internationally. Additionally, this Policy seeks to standardize AML-CFTP procedures within the Company and implement an effective framework to prevent the misuse of its services and products for illicit activities, such as Money Laundering, Terrorism Financing, and the Proliferation of Weapons of Mass Destruction.

3. SCOPE

This Policy applies to the Company and is binding on all its Clients, Employees, Officers, Business Partners, Suppliers, and Third-Party Service Providers, who are required to comply with it in all circumstances.

4. APPROVAL

This Policy and its updates must be formally approved by both the Board of Directors and the Executive Board.

5. EFFECTIVENESS

This Policy shall take effect on the date of its approval and remain in force indefinitely. It should be updated as necessary due to changes in the Internal Risk Assessment (IRA) and/or the processes described herein, or as a result of applicable regulatory requirements.

6. PRINCIPLES

6.1 Internal Risk Assessment

The Company's Internal Risk Assessment (IRA) should be conducted to identify, measure, and mitigate the risk of its products and services being used for Money Laundering and Terrorism Financing. The assessment should consider at least the following risk profiles:

- Clients;
- The institution, including its business model and geographic area of operation;
- Operations, transactions, products, and services, covering all distribution channels and the use of new technologies; and
- Activities carried out by Employees, Partners, and Third-Party Service Providers.

Based on this assessment, the Risk-Based Approach (RBA) methodology is applied, which establishes processes, controls, and procedures that ensure, with respect to Money Laundering and Terrorism Financing risks: (i) identification and assessment, (ii) definition of criteria for prioritizing management actions directed at the most critical or significant risks, (iii) development of responses through the adoption of proportional preventive and mitigation measures for the identified risks, and (iv) ongoing monitoring of conditions and contexts that allow the risk assessment to be updated whenever necessary.

The IRA must be reviewed every two (2) years, as well as whenever significant changes occur in the risk profiles mentioned above.

6.2 Effectiveness Assessment

The effectiveness of the Company's AML-CFTP policies, standards, procedures, and internal controls should be assessed annually to ensure compliance with the Company's responsibilities.

Following the issuance, review, and validation of the improvement areas identified in the Effectiveness Assessment, the Legal and Compliance Department will develop action plans to monitor, in coordination with the business, defense, or governance areas, the implementation of corrective actions to address the deficiencies identified in the report. The action plans should be submitted to the Executive Board for acknowledgment.

6.3 Risk-Based Approach (RBA)

The Company adopts a Risk-Based Approach (RBA), established through the assessment of risk categories and variables. This approach ensures that the measures taken to prevent or mitigate Money Laundering and Terrorism Financing are proportionate to the risks identified during onboarding and throughout the course of the business relationship.

The RBA allows for the application of proportionate measures and controls, ensuring the more efficient allocation of resources and efforts.

7. ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM AND THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION PROGRAM

This Policy establishes a compliance program aligned with current AML-CFTP laws and regulations. It includes a set of actions based on a Risk-Based Approach (RBA), designed to ensure that the Policy is consistent with the risk profiles of the Company's business model, Clients, operations, transactions, products, services, as well as Employees, Partners, and Third-Party Service Providers.

The AML-CFTP Program and its associated processes are designed to ensure adherence to the guidelines set forth in this Policy, in compliance with applicable regulations and Internal Procedure Manuals, and to prevent the misuse of the Company's products and services for illicit activities.

To implement the AML-CFTP Program, the following areas must be addressed:

7.1 Policy, Standards, and Procedures

The Company has established policies, standards, and procedures that comply with local laws and regulations, addressing AML-CFTP measures based on the risk profiles of the business model, Clients, operations, transactions, products and services, as well as Employees, Business Partners, and Third-Party Service Providers. These documents are reviewed periodically, in accordance with the established approval process and review periods.

7.2 Identification, Qualification and Classification

This refers to the set of actions adopted by the Company to identify, qualify, and classify Clients, Suppliers, Partners, and Employees, in compliance with current legislation. These actions include capturing, verifying, validating, updating, and storing registration information.

The Company adopts procedures aimed at knowing its Clients (KYC), Suppliers (KYS), Partners (KYP), and Employees (KYE), from the beginning of the relationship and throughout its entire cycle, in order to mitigate the risk of engaging with individuals potentially involved in ML-CFTP practices.

These procedures are designed to ensure the identification, qualification, and risk-based classification, considering AML-CFTP aspects in line with the Internal Risk Assessment (IRA) and Risk-Based Approach (RBA).

Registration information is periodically updated based on current legislation and the risk criteria outlined in the Internal Risk Assessment.

The Company establishes management and enhanced monitoring procedures for relationships classified as high risk for AML-CFTP purposes.

Restrictive measures are applied when establishing or maintaining relationships with Clients, Suppliers, Partners, and Employees who may potentially be involved in ML-CFTP activities.

The Company also implements procedures and internal controls for relationships involving PEPs and RCAs, taking their condition into account when determining risk classification and evaluating the decision to initiate or maintain the relationship.

Additionally, the Company adopts procedures and internal controls for situations where it is not possible to verify the Ultimate Beneficial Owner.

7.3 Monitoring, Selection, Analysis, and Reporting of Suspicious Transactions or Situations

All transactions and operations carried out by Clients must be continuously monitored through computerized systems, with parameterized alerts to identify situations that may indicate signs of Money Laundering or Terrorism Financing, in accordance with the requirements and timelines established by applicable regulations. These alerts must be verifiable for both their adequacy and effectiveness.

In line with the Risk-Based Approach (RBA), Clients with greater exposure to ML-CFTP risks must be subject to more stringent monitoring and/or enhanced scrutiny of their activities.

The analysis of generated alerts is performed centrally by the Company's AML-CFTP area and formalized through a case file. These activities are not outsourced, except for the hiring of auxiliary services, as permitted by applicable regulations.

The decision to report suspicious transactions or situations to the competent regulatory authorities is the responsibility of the AML-CFTP Deliberative Forum, which meets periodically and may be convened extraordinarily whenever necessary. The Forum has the authority to escalate cases considered particularly sensitive or that may represent a significant reputational risk, in accordance with the Company's approval matrix.

Reports are submitted in compliance with applicable regulations, and those made in good faith do not entail civil or administrative liability.

7.4 Record Keeping and Maintenance of Data and Transactions

All information related to registrations, operations, products, and services provided by the Company must be retained either in its original form or as electronic records, in accordance with the retention periods, responsibilities, and data requirements set forth by applicable laws and regulations.

7.5 Evaluation of New Products and Services

New products and services, including the introduction of new technologies, must be preemptively evaluated in accordance with internal procedures to identify and assess any potential risks of facilitating Money Laundering and/or Terrorist Financing.

7.6 Sanctions

The Company prohibits the initiation or maintenance of relationships with individuals or entities listed on national or international sanctions lists. The Company exercises due diligence to ensure that transactions are not conducted with parties or counterparties subject to sanctions imposed by different countries or external/internal agents, in accordance with national and international best practices.

Additionally, the Company adheres to measures outlined in the sanctions resolutions of the United Nations Security Council (UNSC), which require the freezing of assets or any funds owned, directly or indirectly, by individuals, legal entities, or organizations, as provided by law, without prejudice to compliance with judicial orders or requirements arising from local legislation.

7.7 Training and Promotion of Organizational Culture

To enhance knowledge and maintain ongoing engagement with AML-CFTP topics, the Company periodically develops training programs, which include communication initiatives and/or training sessions for all eligible Employees, Partners, and Third-Party Service Providers. These programs highlight the importance of AML-CFTP issues in relation to corporate responsibilities, legal and regulatory obligations, and the Company's institutional AML-CFTP policies, in accordance with established procedures.

The AML-CFTP training and communication program should be implemented through institutional actions across all areas of the Company, including in-person or online courses (e-learning), workshops, campaigns, notices, publications, and other knowledge dissemination methods.

The Training and Communication Program should also include targeted actions to ensure commitment to AML-CFTP matters at all levels of the Company, including the Executive Board. This reinforces the Company’s institutional values and organizational culture through strategic AML-CFTP initiatives.

8. ROLES AND RESPONSIBILITIES

StoneCo Board of Directors

- Approve this Policy.

Executive Management

- Approve this Policy;
- Acknowledge the Internal Risk Assessment and the Effectiveness Assessment, along with the action plan to address identified deficiencies;
- Commit to the continuous effectiveness and improvement of policies, rules, procedures, and internal controls related to AML-CFTP (Anti-Money Laundering, Countering the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction), and ensure a governance structure that guarantees compliance with these requirements.

Risk Forum

- Advise the Executive Board, which is responsible for deliberating on matters related to Risk Management delegated to it;
- Assist the Risk Management Director in the performance of their duties;
- Support the Legal and Compliance Department in decisions necessary for the proper governance of the AML-CFTP Program;
- Support the AML-CFTP Deliberative Forum whenever requested.

Legal and Compliance Department (AML Area - Director responsible for ensuring compliance with AML-CFTP regulations)

- Ensure the implementation of the AML-CFTP Program;
- Prepare and approve the Internal Risk Assessment;
- Prepare the Effectiveness Assessment and Action Plan Report;
- Define guidelines and minimum criteria for classifying Money Laundering and Terrorism Financing risks for Clients, Employees, Business Partners, Suppliers, and Third-Party Service Providers;
- Ensure compliance with legal and regulatory requirements related to AML-CFTP;
- Develop, update, and maintain the Policy and related documents in adherence to applicable laws and regulations, as well as in line with national and international best practices;
- Technically specify and validate training and continuous education programs for all Employees on AML-CFTP;
- Monitor and select operations and situations with indications of ML-CFTP through automated systems, in compliance with the requirements and timelines established by applicable regulations, and analyze generated alerts, formally documenting them in a technical case file;
- Lead the AML-CFTP Deliberative Forum in decision-making on cases requiring reporting to the FIU and/or client offboarding;
- Ensure the reporting of suspicious transactions to the competent regulatory authorities within the deadlines and terms established by current regulations;
- Submit the “non-occurrence” communication as required by COAF.

Fraud Prevention (Risk Management)

- Ensure the implementation of the Fraud Prevention Program;
- Ensure proper procedures for verifying the Client’s identity at the beginning of their relationship with the company;
- Report any unusual situations related to money laundering or terrorism financing to the AML-CFTP area.

Technology

- Manage, maintain, and improve the IT systems used in AML-CFTP processes overseen by the Risk Technology team;

- Analyze the legal and regulatory AML-CFTP requirements communicated by the Legal and Compliance Department and assess their respective impacts on the systems managed by the Risk Management Platform;
- Report to the Legal and Compliance Department any internal policy updates that require attention or entail systemic development of new guidelines.

Internal Audit

- Perform audit tests and procedures related to AML-CFTP;
- Oversee and verify the full adoption and implementation of the guidelines outlined in this Policy and its related regulations;
- Assess the effectiveness of the Company's processes and controls, as well as the compliance of activities carried out with laws and standards related to AML-CFTP;
- Monitor remediation actions arising from each Internal Audit, External Audit, Internal Controls, and Regulatory reviews;
- Acknowledge the Internal Risk Assessment and the Effectiveness Assessment, along with the associated action plans intended to address the identified deficiencies.

Risk Management

- Support business areas (first line of defense) in assessing operational risks and processes, and in validating the design of controls and action plans;
- Ensure compliance with applicable internal and external regulations, particularly those related to internal control systems;
- Monitor and report on the quality of operational controls through testing and performance indicators.

Compliance

- Ensure the necessary independence, autonomy, and authority for the effective execution of Compliance activities, with direct reporting to the Executive Management to communicate events, failures, and any irregularities that may impact the management of Compliance Risk, as well as the corresponding remediation action plans;
- Ensure the implementation of corrective measures for any identified compliance failures.

Integrity

- Execute compliance controls and monitor employee participation in AML-CFTP training programs;
- Receive, assess, and share reports of suspected Money Laundering and/or Terrorism Financing with the AML-CFTP department.

Employees

- Know, understand, and comply with the guidelines set forth in this Policy;
- Participate in the training sessions made available or required, due to the need for deeper

knowledge and skill development in their roles;

- Report any situation, transaction, or proposal suspected of involvement with any type of illicit activity to the Compliance area or through the whistleblowing channel;
- Maintain confidentiality of processes and restricted information.

9. REPORTING AND CONTACT CHANNELS

The AML-CFTP area is responsible for addressing any questions related to the topics covered in this Policy, as well as any matters not explicitly addressed, through the email: governancapld@stone.com.br. Any identified violations of this Policy should be reported to the Company through the Whistleblowing Channel (Orelhão), available at:

- Website: https://www.contatoseguro.com.br/orelhaostone
- Phone: 0800 881 3629
- App: “Contato Seguro” mobile application
- Whatsapp: +55 51 3376-9353

The Company guarantees the confidentiality and anonymity of all information reported, and ensures protection from retaliation for whistleblowers acting in good faith.

10. CONFIDENTIALITY OF INFORMATION

All information related to evidence and/or suspicions of Money Laundering and Terrorism Financing is strictly confidential. Under no circumstances should such information be disclosed to the parties involved. Reports of suspicious activity, as outlined in Circular Letter No. 4,001 of January 29, 2020, are for the exclusive use of regulatory bodies for analysis and investigation.

11. RELATED DOCUMENTATION OR LEGISLATION

- Federal Law No. 9,613/98;
- Federal Law No. 13,260/16;
- Federal Law No. 13,810/19;
- Decree-Law No. 2,848/40;
- Central Bank of Brazil Circular No. 3,978/2020;
- Central Bank of Brazil Circular Letter No. 4,001/2020;
- Central Bank of Brazil Normative Instruction No. 262/2022;
- Central Bank of Brazil Resolution No. 44/2020.

ANNEX I

Acknowledgment of the Institutional Policy on Anti-Money Laundering, Combating the Financing of Terrorism, and the Proliferation of Weapons of Mass Destruction

I hereby acknowledge that I have received, read, and understood the terms of the "INSTITUTIONAL POLICY ON ANTI-MONEY LAUNDERING, COMBATING THE FINANCING OF TERRORISM, AND THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (AML-CFTP)," and I commit to fully complying with it in the course of my professional activities. I further commit to report any instances of non-compliance with this Policy to the Whistleblower System (ORELHÃO) should I become aware of them, understanding that failure to do so may result in appropriate administrative and legal actions, both during my employment and, where applicable, thereafter.

Acknowledgment by Stone Employees

Full Name: **CPF (Individual Taxpayer ID):**

Signature: **Location and Date:**

Date: _____/_____/_____