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

APPROVAL	
Approval Date	**Approved by**
19/12/2024	StoneCo Board of Directors StoneCo Executive Board

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

INDEX

1. TERMS AND DEFINITIONS

AML-CFTP: Stands for Anti-Money Laundering, Countering the Financing of Terrorism, and the Proliferation of Weapons of Mass Destruction.

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

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.

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

CBB: Stands for the Central Bank of Brazil.

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

COAF: Stands for the Financial Activities Control Council (Conselho de Controle de Atividades Financeiras), the Brazilian financial intelligence unit established by Law No. 9,613, dated 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, including biological, chemical, or nuclear weapons.

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 Board: Refers to the Executive Board of StoneCo 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, movement, or ownership of assets, rights, or values derived, directly or indirectly, from illegal activities. These practices are typically carried out through transactions designed to obscure the illegal source 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 parties 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 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, either national or foreign, who holds a prominent public position, as well as their close associates, including representatives, family members, or close collaborators, as outlined in Article 27 and further clarified in Article 19 of Circular No. 3,978, dated January 23,2020.

Policy: Refers to this Institutional Policy on Anti-Money Laundering , Countering the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction (AML-CFTP).

Prestadores de Serviços Terceirizados ou **Terceiros:** significa a entidade, seu representante legal e/ou preposto que prestem ou estejam prestando serviços terceirizados para a Companhia.

RBA: stands for "Risk-Based Approach", a methodology used to better allocate efforts and resources in the implementation of AML-CFTP practices.

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. The company is registered with the Brazilian Taxpayer ID (CNPJ/MF) under No. 31.752.270/0001-82.

Terrorist Financing: Refers to the process of structuring financial sources (whether legal or illegal) that are moved in a concealed or disguised manner to fund terrorist activities and/or groups.

UNSC: Stands for the United Nations Security Council.

2. OBJECTIVES

This Policy aims to establish the Company's principles and framework for preventing Money Laundering, Terrorist 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 for illicit activities, such as Money Laundering and Terrorist Financing.

3. SCOPE

This Policy applies to the Company and is binding on all Clients, Employees, and Administrators of StoneCo, as well as its business Partners, Suppliers, and Third-Party Service Providers. All parties are required to adhere to this Policy in all circumstances.

4. APPROVAL

This Policy, along with any updates, must be formally approved by both the Board of Directors and the Executive Board of StoneCo.

5. EFFECTIVENESS

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

6. PRINCIPLES

6.1 Internal Risk Assessment (IRA)

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

- Clients;
- The institution, including its business model and geographical scope;
- 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 to ensure that preventive and mitigating measures for Money Laundering and Terrorist Financing are proportionate to the identified risks.

The IRA should be reviewed every two (2) years or whenever significant changes occur in any of the aforementioned risk profiles.

6.2 Effectiveness Assessment

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

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

6.3 Risk-Based Approach (RBA)

The Company adopts a Risk-Based Approach (RBA), which is determined through the evaluation of various categories and variables. This ensures that the measures taken to prevent or mitigate Money Laundering and Terrorist 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 legislation and regulations. It includes a set of actions based on a Risk-Based Approach, 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 Policies, 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 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 implements Know Your Client (KYC), Know Your Supplier (KYS), Know Your Partner (KYP), and Know Your Employee (KYE) procedures from the beginning of the relationship and throughout its duration, aiming to mitigate the risk of engaging with individuals potentially involved in Money Laundering and Terrorist Financing activities (ML/TF).

The procedures are designed to ensure the identification, qualification, and classification of these entities. Classification is based on risk levels, considering AML-CTF factors and in alignment with the Internal Risk Assessment.

Registration data is updated periodically, in accordance with applicable legislation and the risk criteria outlined in the Internal Risk Assessment.

The Company applies management and monitoring procedures for relationships identified as High Risk for AML-CTF purposes.

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

The Company also implements procedures and internal controls for relationships involving Politically Exposed Persons (PEPs), taking their PEP status into account when determining risk classification and evaluating the decision to initiate or maintain the relationship. The procedures extend to representatives, family members, and close associates of these individuals.

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

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

All transactions and operations conducted by Clients must be continuously monitored using system-generated alerts to detect potential Money Laundering (ML) or Terrorist Financing (TF) activities, in accordance with the requirements and timelines set by applicable regulations. These alerts must be verifiable for both their adequacy and effectiveness.

In line with the Risk-Based Approach, Clients deemed to have higher exposure to ML/TF risks will be subject to more stringent monitoring and/or enhanced scrutiny of their activities.

Any operations or proposals showing signs of potential Money Laundering or Terrorist Financing must be reported to the relevant regulatory authorities, in accordance with the procedures established by applicable regulations. Reports made in good faith will not result in civil or administrative liability.

7.4 Record Keeping and Maintenance of Data and Transactions

All information related to client registration, transactions, and the products or services provided by the Company will 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 continuation 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 various countries or external/internal authorities, in accordance with best national and international practices.

Furthermore, 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 listed in these resolutions. This is done in accordance with legal provisions, without prejudice to compliance with judicial orders or local laws.

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-CFT (Anti-Money Laundering / Combating the Financing of Terrorism), and ensure a governance structure that guarantees compliance with these requirements.

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

- Ensure the implementation of the AML-CFT Program;
- Develop and approve the Internal Risk Assessment;
- Prepare the Effectiveness Assessment and Action Plan Report;
- Establish guidelines and minimum criteria for assessing money laundering and terrorism financing risks related to Clients, Employees, Business Partners, Suppliers, and Third-Party Service Providers;
- Ensure compliance with all legal and regulatory requirements related to AML-CFT;
- Develop, update, and maintain the Policy and related documents in alignment with applicable laws, regulations, and best practices, both nationally and internationally;
- Design and validate ongoing training and education programs for all employees on AML-CFT.

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-CFT area.

Technology

- Manage, maintain, and improve the information system(s) used in AML-CFT processes managed by the Risk Technology team;
- Analyze legal and regulatory AML-CFT requirements provided by the Legal and Compliance

Department and evaluate their impact on systems managed by the Risk Management Platform;
- Report any internal policy changes that require attention or the development of new system guidelines to the Legal and Compliance Department.

Internal Audit
- Conduct regular testing in line with the company's internal controls in AML-CFT;
- Oversee and verify the full adoption and implementation of the guidelines outlined in this Policy and its related regulations;
- Evaluate the effectiveness of the company's processes and controls, ensuring compliance with AML-CFT laws and regulations;
- Monitor the resolution of issues raised by the Internal Audits and Regulatory inspections;
- Review the Internal Risk Assessment and Effectiveness Assessment, along with the associated action plans to address 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.

Risk Forum
- Advise Executive Management on matters related to Risk Management delegated to it;
- Assist the Director of Risk Management in their duties;
- Support the Legal and Compliance Department in decision-making related to the governance of the AML-CFT Program.

Integrity
- Implement controls to ensure employee adherence to AML-CFT training programs;
- Receive, assess, and share any reports of suspected money laundering or terrorism financing with the AML-CFT area.

Employees

- Understand and comply with the guidelines of this Policy, including participation in required training to enhance their knowledge and competence in their roles;
- Report any suspicious situations, operations, or proposals potentially linked to illicit activities to the Compliance department or through the whistleblower system (Orelhão);
- Maintain confidentiality of all processes, confidential information and restricted data.

9. REPORTING AND CONTACT CHANNELS

The AML-CFT department is responsible for addressing any questions related to the topics covered in this Policy, as well as any matters not explicitly addressed. Any identified violations of this Policy should be reported to the Company through the Whistleblower System (Orelhão), available at:

- canalconfidencial.com.br/orelhaostone
- Phone: 0800-591-0579

The Company ensures the confidentiality and anonymity of all information reported, and guarantees 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-CFT)," 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: _____/_____/_____