Anti-Money Laundering Policy

Code	PO.COMP.002
Version	V.3
Publication	09/12/2022
Elaborated by	Compliance Team
Data Classification	Public
Disclosure	External

Content

1. Introduction 2

2. Important Definitions 2

3. Financing Terrorism 3

4. Politically Exposed Person (PEP) 3

5. Operational Principles 5

6. Red Flags for Money Laundering and Terrorist Financing 6

7. Enhanced Due Diligence 7

8. Insider Abuse 7

9. Seeking Advice and Reporting Potential Violations 8

10. Policy Review 8

11. History 9

1. Introduction

VTEX (“Company”) is committed to conducting its business with the highest ethical and legal standards and expects all employees and other individuals acting on its behalf to uphold this commitment. As such, the Company has adopted this Anti-Money Laundering Policy (“Policy”), which applies to all directors, officers, employees, agents, representatives, consultants, advisors, distributors, supplier contractors, or other third parties acting on behalf of the Company, even on a provisional and temporary basis ("Company Personnel").

VTEX will not conduct business with individuals or corporations whose conduct may raise suspicions of involvement with illegal activities. VTEX will report any suspicions of money laundering or terrorist financing activity to the relevant authorities.

This Policy and the internal controls herein have been designed to avoid money laundering, including the laundering of illicit proceeds by the same person (self-laundering) and the use of money, goods, or gains of illicit provenance and, consequently, prevent the potential criminal liability of the Company that could result from such violations/crimes.

Company Personnel who violate this Policy may be subject to disciplinary action, including dismissal from the Company, termination of agreements, and or any other associated legal and out-of-court actions, in accordance with the applicable law. The consequences for violating anti-money laundering laws can be severe for the Company, including significant fines, loss of operating licenses, limitations on engaging in certain business activities, imprisonment, and reputational damage.

The Company Personnel must comply with the anti-money laundering laws of all countries where the Company operates.

2. Important Definitions

Money laundering is defined as engaging in acts to conceal or disguise the origins of illegally or criminally derived proceeds and assets so that they appear to have legitimate origins and are introduced into the legal financial and business as if they were lawful. If any Company Employee or Company Personnel suspects that there has been money laundering, that person must immediately report the suspected violation to VTEX’s Compliance Team.

Under this Policy, the following conducts shall be regarded as money laundering:

- The conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, with the purpose of concealing or

disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action.

- The concealment or disguise of the true nature, source, location, position, movement, and rights concerning to, or ownership of, property, knowing that such property is derived from criminal activity or an act of participation in such activity.
- The acquisition, possession, or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or an act of participation in such activity.
- Participation in, association to commit, attempts to commit, and aiding, abetting, facilitating, and counseling the commission of any of the above-mentioned actions.

Examples of illicit provenance are forgery of money, extortion, robbery, drug crime, fraud, corruption, organized crime, terrorism, etc.

The money laundering process consists of three “stages”:

1) **Placement:** This involves introducing illegally obtained money or other valuables into financial or non-financial institutions.
2) **Layering:** Layering occurs by conducting multiple, complex financial transactions that make it difficult to link the money to illegal activity. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.
3) **Integration:** Placing the laundered proceeds back into the economy so that they re-enter the financial system as apparently legitimate funds.

3. Financing Terrorism

Company Personnel must immediately report any suspected or known terrorist financing to VTEX’s Compliance Team. For the purposes of this Policy, “terrorist financing” means the provision or collection of funds by any means, directly or indirectly, with the intention to be used or in the knowledge that they are to be used, in full or in part, to use indiscriminate violence as a means to create terror, fear, or to achieve a political, religious, or ideological aim.

4. Politically Exposed Person (PEP)

Transactions involving Politically Exposed Persons (“PEPs”) require enhanced due diligence. A PEP is an individual who is or has been entrusted with a prominent public function. Due to their position and influence, it is recognized that many PEPs are in positions that potentially can be abused to commit

money laundering offenses and related predicate offenses, including corruption and bribery, as well as conducting activity related to terrorist financing. The potential risks associated with PEPs justify the application of additional anti-money laundering/counter-terrorist financing preventive measures.

For the purposes of this Policy, Politically Exposed Persons ("PEP") include, but are not limited to:

- Heads of State, heads of government, ministers, and deputy or assistant ministers.
- Members of parliament or similar legislative bodies.
- Members of the governing bodies of political parties.
- Members of supreme courts, of courts, or other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances.
- Members of courts of auditors or the boards of central banks.
- Mayors and members of local administration, city, and district assemblies.
- Ambassadors, chargée d'affaires, and high-ranking officers in the armed forces.
- Members of the administrative, management or supervisory bodies of State-owned enterprises.
- Directors, deputy directors, and members of the board or equivalent function of an international organization.

Not only the person that officiates a public function must be considered as PEP, but also close family members must be included in the assessment. For the purpose of this Policy, family members mean:

- The spouse, or a person considered equivalent to a spouse, of a politically exposed person.
- The children and their spouses, or persons considered equivalent to a spouse, of a politically exposed person.
- The parents of a politically exposed person.

Also, persons known to be close associates to a PEP must be assessed with the same risk approach, such as:

- Natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a Politically Exposed Person.
- Natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a Politically Exposed Person.
- Natural persons who have close relationships with a PEP in a social way, such as known sexual partners outside the family unit (e.g. boyfriend, girlfriend, etc.).

5. Operational Principles

The careful examination of those operations where risk factors exist is important. For example, this could mean those in which third parties propose the use of cash or bearers' checks, international transactions (in particular those with persons or entities residents in tax havens or high-risk territories, or different locations from those where the company operates), operations with persons holding positions of public responsibility or PEPs or transactions conducted through or related to intermediary companies.

The Company Personnel should not initiate, maintain or accept a new business relationship (customer, supplier, financier, etc.), provide services or take action with anyone known or suspect to be involved in money laundering or terrorist financing, even if in different businesses from the relationship being established with VTEX.

Likewise, the Company Personnel should not deal with money, goods, or valuables that they are aware of or suspect to be from an illicit origin or that they are unaware of.

VTEX is committed to fighting against money laundering and the financing of terrorism. Therefore, the following due diligence principles should be followed, not only in situations where particular risk factors exist, but as to all customers and third parties:

1) Identifying the Third Party

The Company must conduct due diligence on customers and other third parties and document the findings. As part of the due diligence process, the following minimum information should be collected:

(i) for Brazilian targets - National Registry of Legal Entities ("CNPJ") for entities or TAX ID ("CPF") of the person providing services or goods;

(ii) for International targets - Full legal name of the Company and its partners with more than 10% of participation or full legal name of the individual. Also, if deemed necessary, the Company can request additional information in order to better assess and mitigate integrity and money laundering risks.

As part of due diligence, the Company must verify that the customer or third party does not appear on any of the US Department of the Treasury Office of Foreign Assets Control's sanctions list, including the Specially Designated Nationals and Blocked Persons lists, as well as if the client or the third party is responding or has already responded to the Administrative Sanctioning Process (PAS) by the Financial Activities Control Council (COAF) or is included in the National Register of Punished Companies (CNEP), of the Federal Government of Brazil. The Company should ask and search to confirm, whether the client or third party is or has been involved in an investigation of any kind involving corruption, money laundering or acts of terrorism. The Company will not enter into a business relationship with a person or an entity that appears on one of these lists.

The Company must also take steps to understand the nature and purpose of the customer or third-party relationship and develop an appropriate risk profile based on the information learned. Based on the risk profile, the Company may actively maintain and update the customer or third-party information. The Company also will conduct ongoing monitoring to identify suspicious transactions and report those transactions where legally required.

2) Identifying the Ultimate Beneficial Owner (UBO)

Before the commencement of a commercial relationship, whether of a habitual nature, and prior to its execution, the Ultimate Beneficial Owner of any Third Parties who are formally involved must be identified. The Company must document this analysis. Ultimate Beneficial Owner (UBO) means the person who directly or indirectly controls 25% or more of the equity or voting rights in the corresponding company or owns the company. In the event of the existence of a beneficial owner in the third party, that person must be identified through their name, nationality, National Identity Number (RG), passport, Foreigner's Identity Number (RNE), or residence card. Listed companies are excluded from the obligation to identify the UBO.

If the UBO is a PEP, then the Company must conduct enhanced due diligence before entering into any contractual or commercial relationship with the entity.

3) Obligation to formally record commercial relationships in writing

Before the commencement of commercial relationships and prior to carrying out transactions with third parties (attention being paid to those of an international nature), the relationship must be formally recorded in a written agreement in accordance with VTEX's standards.

The provisions in a written agreement should include a commitment to comply with the Anti-Money Laundering laws and VTEX's right to immediately terminate the contract in case of violation, subject to applicable law.

6. Red Flags for Money Laundering and Terrorist Financing

Red Flags for Money Laundering and Terrorist Financing include:

- Unexplained spikes in account activity.
- Large number of transactions, which could indicate layering.
- The third party tries to conceal its identity or the source of its funds.

- The third party is an entity without a clear registered office and does not appear online.
- The third party's structure makes it difficult to recognize it.
- The third party funds for the transaction come from abroad when there is no apparent link between the country where the funds are sourced and the third party.
- The third party uses multiple bank accounts or ones held abroad without any justification.
- The third party intends to make payments in cash or using bearer checks.
- The third party intends to pay a higher price for the services for no good reason.
- The third party is based in a tax haven or a high-risk country.

7. Enhanced Due Diligence

If you identify a red flag or the transaction directly or indirectly involves a PEP, then enhanced due diligence must be conducted prior to entering into a business relationship with the customer or third party.

Enhanced due diligence involves the gathering of additional information to ensure that the person or entity is not participating in any improper or illicit conduct. This information should include, but is not limited to, the source of the funds, the source of the individual or company's wealth, and the individual's occupation or the type of business. The findings of enhanced due diligence should be documented.

If you are unsure whether enhanced due diligence is required in a particular situation or have any other questions regarding enhanced due diligence, you should contact VTEX's Compliance Team.

8. Insider Abuse

Company Personnel and other individuals that are closely affiliated with the Company should not also engage in actions that constitute money laundering or facilitate the commission of money laundering.

If you suspect that an employee or other Company affiliate has engaged in improper or illicit activity, or if you have any questions about insider abuse, you should contact VTEX's Compliance Team.

VTEX has zero tolerance for any form of retaliation, including intimidation, exclusion, humiliation, or other forms of harassing employees who, in good faith, report misconduct or express concern about a particular practice or decision.

The Ethics Channel is a safe way to receive suspicions or complaints, and anonymity is allowed. If you want to identify yourself, we guarantee secrecy and confidentiality. The Compliance Team, when receiving reports on the Ethics Channel, will maintain confidentiality and, when sending cases to the Ethics Committee, even if the whistleblower has identified himself, his name and any information that may reveal his identity will be hidden.

9. Seeking Advice and Reporting Potential Violations

Company Personnel must immediately report to the Compliance Team the facts or circumstances that may be characterized as a violation of the law or the company's internal policies. If you suspect a violation of this Policy or of any anti-money laundering laws, you must notify a Compliance Team member without delay, and you should not comment on your suspicion or any indication or evidence thatthird-party aware of with any third parties. If you are unsure of whether the conduct constitutes money laundering or have any questions regarding this Policy or other VTEX policy, or if need help or wish to raise a concern, you may communicate that to our Compliance Team or you can use VTEX's Ethics Channel: https://canalconfidencial.com.br/vtex/. Our Ethics Channel is safe and confidential and protects against retaliation.

VTEX has zero tolerance for any form of retaliation, including intimidation, exclusion, humiliation, or other forms of harassing employees who, in good faith, report misconduct or express concern about a particular practice or decision.

10. Policy Review

Any material revision or abolition of this Anti-Money Laundering Policy requires a resolution by the Board of Directors of VTEX.

11. History

Version	Updates
1.0	Elaboration and Approval of VTEX Anti-Money Laundering Policy
2.0	Review of VTEX Anti-Money Laundering Policy
3.0	Review of VTEX Anti-Money Laundering Policy

Elaborated by:

Version	Name	Occupation	Date
1.0	Bruna Flor	People Partner	11/09/2020
2.0	Matheus Vieira	Compliance Analyst	31/05/2021
3.0	Mylla Crespo	Risk and Compliance Intern	04/11/2022
3.0	Pedro Carvalho	Risk and Compliance Senior Analyst	17/11/2022

Reviewed by:

Version	Name	Occupation	Date
2.0	Daniel Agra	Risk and Compliance Manager	31/05/2021
3.0	Daniel Agra	Risk and Compliance Manager	09/12/2022

Approved by:

Version	Name	Occupation	Date
2.0	Thiago Athayde	Risk and Compliance Director	31/05/2021
3.0	Thiago Athayde	Risk and Compliance Director	09/12/2022