ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23 A Publicly-Held Company NIRE 35300010230

PUBLIC DISCLOSURE VERSION

CORPORATE POLICY FOR THE PREVENTION OF UNLAWFUL ACTS

1. OBJECTIVE

To consolidate the principles and guidelines of the Itaú Unibanco Conglomerate to promote a culture of integrity, ethics, and prevention of unlawful acts, including combating money laundering, terrorism financing, proliferation of weapons of mass destruction, corruption, fraud, and claims. This document aims to ensure compliance with current laws and regulations, as well as alignment with national and international best practices.

2. TARGET AUDIENCE

This policy applies to the Itaú Unibanco Conglomerate and its companies in Brazil and abroad.
The requirements of local policies and legislation, where foreign representations are located, must be individually assessed and will follow the guidelines established by the Governance Rule for AML/CFT – International Units (Global).

3. INTRODUCTION

Financial institutions play a central role in preventing unlawful acts such as money laundering, terrorism financing, corruption, fraud, and claims. These acts involve the concealment of illegal funds, support for criminal activities, or misuse of financial structures for illicit purposes.

Money laundering seeks to conceal or disguise the criminal origin of assets or funds.

Terrorism financing and proliferation of weapons of mass destruction occur when resources are directly or indirectly allocated to these purposes.

Corruption involves offering or receiving undue advantages to influence decisions or actions.

Fraud refers to deceptive practices aimed at obtaining undue gains.

Claims are unexpected events causing losses, such as robberies, thefts, or kidnappings.

Embargoes and trade restrictions are measures imposed by authorities against countries, companies, or individuals involved in illicit activities.

The challenge lies in identifying and preventing increasingly sophisticated operations that attempt to mask the origin and destination of illegal resources.

Itaú Unibanco, aware of this scenario, maintains a dedicated structure for the prevention of unlawful acts, focusing on governance, transparency, regulatory compliance, and cooperation with authorities.

4. ROLES AND RESPONSIBILITIES

Board of Directors
Approve oversight and prevention guidelines for unlawful acts and monitor evaluation reports and action plans.

Audit Committee
Oversee the corporate program for the prevention of unlawful acts and receive reports from the responsible area for awareness.
Additionally, the Board of Directors and Audit Committee receive the Internal Risk Assessment, Effectiveness Evaluation Report, and the corresponding Action Plan and Follow-up Report.

Senior Compliance and OpRisk Committee

Define the institution's strategic direction in preventing unlawful acts. Key responsibilities include: establishing and proposing prevention guidelines to the Board of Directors; evaluating program results; and deliberating on exceptional situations not covered by the current policy.

Risk and Capital Management Committee
Support the Board of Directors in overseeing Itaú Unibanco's risk and capital management. Also receives the Internal Risk Assessment prepared by the AML Department (DPLD) for awareness.

Anti-Money Laundering Department
Ensure effective implementation of the Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) Program across Itaú Unibanco, both in Brazil and abroad. Key responsibilities include:

- **Risk Management**: Prepares and approves the Internal Risk Assessment, defines classification criteria, and monitors the evolution of money laundering and terrorism financing typologies.
- **Governance and Compliance**: Ensures compliance with the AML/CFT policy, validates business area procedures, and reports relevant facts to the Audit Committee.
- **Prevention and Monitoring**: Assesses risks in new products, services, and technologies, and implements a risk-based approach with effectiveness indicators.
- **Relationships and Partnerships**: Analyzes contracts with foreign financial institutions and third parties in payment arrangements, in accordance with current regulations.
- **AML/CFT Director Responsibilities**: Manages strategic risks, approves the Internal Risk Assessment, delegates operational authority, and monitors critical decisions related to the program.

Fraud Prevention Department
Manage the fraud and claims prevention program, ensuring information integrity and physical security.

Business and Support Units
Implement controls and procedures aligned with corporate guidelines and ensure employee participation in integrity training.

Legal Department
Assist in analyzing legal and regulatory requirements, developing AML/CFT control action plans, and assessing risks in suspicious transactions or operations involving money laundering, fraud, and claims.

Compliance and OpRisk Department
Independently ensure the effectiveness of internal controls through monitoring and effectiveness testing. Reports residual risk, tracks identified deficiencies, and prepares periodic reports in accordance with internal policy and regulations.

Internal Audit
Periodically assess the effectiveness of governance, risk management, and internal controls.

Employees and Administrators
Understand and follow the guidelines and training, and report suspicions of unlawful acts.

5. CORPORATE PROGRAM FOR THE PREVENTION OF UNLAWFUL ACTS

To ensure compliance with the guidelines of this policy and prevent its products and services from being used in illicit activities, Itaú Unibanco has established a Corporate Program for the Prevention of Unlawful Acts. This program must be applied both in Brazil and in International Units and must include at minimum:

5.1. Prevention and Combat of Money Laundering and Terrorism Financing

Policies and Procedures

Itaú Unibanco adopts structured policies and procedures that guide the prevention of unlawful acts, in accordance with legal and regulatory standards. These guidelines consider the risk profile of clients, employees, partners, and operations, promoting proportional and effective actions.

Internal Risk Assessment and Effectiveness Evaluation

This refers to the internal assessment aimed at identifying and measuring the risk of using its products and services for money laundering and terrorism financing. It must also evaluate the effectiveness of the policy, procedures, and internal controls.

The assessment supports the risk-based approach, which guides the application of measures proportional to the severity of identified risks—reinforced for high risks and simplified for lower risks—according to internal guidelines.

The Effectiveness Report includes the methodology used, tests applied, evaluator qualifications, and identified deficiencies. Corrective actions are tracked through a Follow-up Report, ensuring continuous improvement of the program.

Customer Identification

A set of actions aimed at identifying and qualifying customers, their administrators, and representatives through the collection, verification, and validation of essential information to confirm their identity. These data must be updated and stored according to regulatory deadlines.

Full qualification includes verifying Politically Exposed Person (PEP) status and analyzing the corporate chain up to the identification of the ultimate beneficial owner. The guidelines for this process are described in the Corporate Customer Registration Policy.

Know Your Customer – KYC

A set of actions to ensure the identity, economic activity, and origin of customer funds, allowing assessment of their financial capacity and preventing misuse of products and services. The more accurate the information collected at the beginning of the relationship, the more effective the risk and illicit act identification.

Based on a risk-based approach, customers with greater exposure undergo more rigorous analysis.

Complete guidelines are described in internal rules, including the authority to initiate and maintain

relationships with PEPs.

Know Your Partner – KYP

A set of practices aimed at identifying and qualifying commercial partners—legal entities with contractual relationships with Conglomerate companies, according to criteria defined in the Commercial Partnerships Governance Policy.

These partners, including domestic and foreign correspondents, must be classified by risk categories based on their activities. The goal is to prevent relationships with dishonest or illicitly involved counterparts, ensuring they adopt adequate AML/CFT controls. Full guidelines are described in internal rules.

Know Your Supplier – KYS

A set of practices aimed at identifying and qualifying suppliers and outsourced service providers, based on the nature of their activities and the risk associated with the relationship.

These agents must be classified into risk categories, and when higher exposure to unlawful acts is identified, stricter due diligence criteria are applied. The goal is to ensure relationships with counterparts that are ethical and aligned with AML/CFT guidelines. Full guidelines are described in internal rules.

Know Your Employee – KYE

A set of measures aimed at identifying and qualifying employees and candidates, focusing on preventing risks related to money laundering, terrorism financing, and other unlawful acts.

Risk classification considers the roles performed, allowing preventive actions from the selection process to continuous conduct monitoring. The goal is to ensure integrity and security in work relationships. Full guidelines are described in internal rules.

Evaluation of New Products and Services

Prior evaluation of risks related to AML/CFT in new products and services, including the use of new technologies when applicable, must be conducted according to internal guidelines.

Compliance with Sanctions

A set of controls aimed at complying with economic, political, and commercial sanctions imposed by national and international authorities. Includes monitoring of restrictive lists and prohibition of relationships with individuals, entities, or countries involved in illicit activities. Full guidelines are described in internal rules.

Monitoring, Selection, and Analysis of Suspicious Transactions

A continuous process of transaction monitoring based on customer profile and behavior to identify signs of money laundering or terrorism financing. Higher-risk customers are subject to stricter rules and more frequent monitoring.
This process must be conducted independently by the AML/CFT area, separate from commercial areas.

Reporting Suspicious Transactions

Operations, situations, or proposals with signs of money laundering or terrorism financing must be reported to the competent regulatory bodies, when applicable, in compliance with legal and regulatory requirements. Good-faith reports do not result in civil or administrative liability for Itaú Unibanco or its administrators and employees. Information about these reports is restricted and must not be disclosed to customers and/or third parties.

Training and Awareness

The AML/CFT training program promotes continuous education and spreads awareness of the topic, ensuring learning and understanding of its importance, as well as deepening and refreshing knowledge. Training must be provided to administrators, all employees, and eligible commercial partners. Training actions may include in-person or online courses, lectures, campaigns, and other initiatives, according to internal guidelines.

5.2. Prevention and Combat of Fraud

The prevention and combat of fraud are institutional commitments involving all employees, based on principles of ethics, integrity, and compliance. Fraud may occur through:

- Violations of the Code of Ethics and internal rules, such as engaging in practices not authorized by the company, misconduct, breach of confidentiality, and conflicts of interest.
- Non-compliance with legal and regulatory obligations that jeopardize the organization's image, assets, or continuity.
- Unlawful acts such as forgery, fraud, embezzlement, theft, robbery, and extortion.

Preventive actions aim to identify inappropriate behavior, mitigate risks, and protect the organization, its clients, and partners from financial, operational, and reputational losses.

Risk Assessment at the Beginning of the Relationship

Service and product contracting processes must include procedures to prevent and mitigate fraud risk at the beginning of the relationship with applicants.

Prevention and Combat of Internal Fraud

Itaú Unibanco adopts specific measures to prevent fraud involving its employees, through guidelines and control procedures for the prevention and detection of irregular activities.

Prevention and Combat of Accounting Fraud

Itaú Unibanco adopts specific measures to prevent accounting fraud, through guidelines and control procedures for the prevention and detection of irregular activities.

Risk Assessment in New Products and Services

New products and services must be evaluated in advance from a fraud prevention perspective, according to internal guidelines.

Transaction Monitoring

Products and services contracted by clients must be monitored to detect and investigate unusual or suspicious situations involving fraud or other unlawful acts.

Handling of Incidents

Suspected or confirmed situations must be investigated to determine responsibilities and necessary actions. Procedures and decisions taken during incident handling must be documented to support legal proceedings.

Training and Awareness

The training program is continuous and aimed at strengthening the culture of integrity and prevention of fraud and claims. Its objectives include deepening employees' regulatory knowledge and enabling them to identify, prevent, handle, and report suspicious situations.

Training actions are promoted institutionally and within business units through in-person and online courses, lectures, campaigns, and other knowledge dissemination methods.

6. INFORMATION AND RECORD RETENTION

All information and records related to unlawful acts must be retained according to the timeframes established by applicable legislation.

7. TRANSPARENCY IN CLIENT RELATIONSHIPS

Clients have easy access to their financial information through various channels, making them important allies in the prevention of unlawful acts. Additionally, they are continuously informed about risks and precautions through relationship channels.

8. REPORTING CHANNELS FOR UNLAWFUL ACTS

Administrators, employees, partners, and outsourced service providers of Itaú Unibanco must, within the scope of their responsibilities, immediately report proposals or occurrences of situations or operations with signs or evidence of unlawful acts identified during prospecting, negotiation, or ongoing relationships using the following established channels, either physically or electronically:

Situations Related to Money Laundering or Terrorism Financing
In Brazil, reports must be sent to the AML Department (DPLD):

- Internal Channel: IU Conecta > Utilities > PLD Online
- Website:https://www.itau.com.br/atendimento-itau/para-voce/denuncia/

In international units, reports must be sent to local channels or the Unit's Compliance Officers.

Situations Related to Fraud and Other Unlawful Acts
In Brazil, reports must be sent to the Fraud Inspection and Prevention Superintendency or the Audit Committee:

Fraud Inspection and Prevention Superintendency
- CHAT: PF > EA > Relationship > Chat > Inspection
- CHAT: PJ > Via Iris icon on Teams or https://itau.service-now.com/tech
- Website: www.itau.com.br/atendimento-itau/para-voce/denuncia
- External email: inspetoria@itau-unibanco.com.br

In international units, reports must be sent to local channels or the Unit's Compliance Officers.

Audit Committee
- External email: comite.auditoria@itau-unibanco.com.br
- Mailing address:
A/C Audit Committee of Itaú Unibanco Holding S.A.
Praça Alfredo Egydio de Souza Aranha, 100
Olavo Setubal Tower – PT Floor
ZIP Code 04344-902 – São Paulo – SP

These channels must be disclosed and may also be used by clients, service providers, and the general public.

9. WHISTLEBLOWER PROTECTION

Whistleblower protection is an essential principle to ensure the integrity of the corporate environment.
Any form of retaliation against those who, in good faith, report suspicions or violations of policy guidelines is strictly prohibited. Reports may be anonymous, and the confidentiality of information must be preserved throughout the investigation process. Disciplinary sanctions will be applied both to those who retaliate and to those who act in bad faith by making unfounded reports. Anonymous reports can be made through the website: www.itau.com.br/atendimento-itau/para-voce/denuncia

10. APPLICABLE SANCTIONS

Failure to comply with legal and regulatory provisions subjects administrators and employees to sanctions ranging from administrative penalties to criminal charges for money laundering, terrorism financing, fraud, corruption, and other unlawful acts.

Negligence and Voluntary Failure are considered violations of this policy, the Code of Ethics, and the Corporate Policy on Integrity, Ethics, and Conduct, and may result in disciplinary measures as defined in the Guidelines for Disciplinary Measures.

11. INFORMATION SHARING

When applicable and in accordance with the information security guidelines established in the Corporate Information Security and Cyber Security Policy, information exchange may occur between control areas to comply with the guidelines established in this policy.

12. RELATED REGULATIONS

This policy must be read and interpreted in conjunction with the following documents:

Banco Central do Brasil Circular Letter No. 4,001/2020
Banco Central do Brasil Circulars No. 3,691/2013, 3,680/2013, and 3,978/2020 and their amendments
Superintendência de Seguros Privados Circular No. 612/2020 and its amendments
Brazilian Penal Code – Decree-Law No. 2,848/1940
Superintendência Nacional de Previdência Complementar Instruction No. 34/2020
Law No. 12,846/2013
Law No. 9,613/1998 and its amendments
Law No. 13,810/2019 and related laws
SARB Self-Regulation Standard No. 011/2013 – Brazilian Federation of Banks
Recommendations from the Financial Action Task Force (FATF)
Resolution No. 021/2012 – Council for Financial Activities Control
Resolution No. 50/2021 – Brazilian Securities and Exchange Commission and its amendments
Resolutions No. 4,567/2017 and 4,753/2019 – National Monetary Council
Wolfsberg Anti-Money Laundering Principles

13. GLOSSARY

Unlawful Acts: All conscious human actions or omissions aimed at committing criminal offenses—money laundering, terrorism financing, corruption, and fraud.

Close Associates: Individuals known to have a close relationship with a politically exposed person (PEP), including: i) joint participation in a private legal entity; ii) acting as a proxy, even via private instrument; iii) joint participation in non-legal arrangements; Also includes individuals controlling entities or arrangements created for the benefit of a PEP.

Ultimate Beneficial Owner: The individual who ultimately controls a legal entity or on whose behalf a transaction is conducted. Also includes representatives, proxies, or agents who effectively command the activities of a legal entity client.

Special Attention: Situations requiring enhanced monitoring.

Voluntary Failure: Intentional involvement in unlawful actions, such as structuring or advising others to structure operations to evade regulatory reporting, or knowingly engaging in transactions involving illicit funds.

Itaú Unibanco: Itaú Unibanco Holding S.A.

Politically Exposed Persons (PEPs): Public officials who currently hold or have held, within the last five years, positions, jobs, or public functions in Brazil or abroad, as defined by regulatory bodies, including their representatives, direct or collateral relatives, and close associates. Legal entities whose representatives or controllers are PEPs are also subject to enhanced due diligence.

AML/CFT: Anti-Money Laundering and Counter-Terrorism Financing and Proliferation of Weapons of Mass Destruction.

Focal Points: Administrators or employees appointed by the business unit executive to ensure compliance with corporate AML/CFT guidelines.

Retaliation: Acts of persecution, revenge, or punishment against administrators or employees who raise concerns, suspicions, or findings. Examples include threats, demotion, blacklisting, suspension, or dismissal.

Claim: Unusual events causing losses or disasters to Itaú Unibanco, such as branch or client robberies, kidnapping for extortion, thefts, accidents, break-ins, etc.

Approved by the Board of Directors on 2025, September.