AML/CFT/WMD Risk Prevention Policy

05-05-2025

1. PURPOSE

The purpose of this policy is to establish the principles, guidelines, and procedures that support the institutional commitment of Contacto to prevent, detect, control, and report activities related to Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT), and the Proliferation of Weapons of Mass Destruction (WMD).

Its application seeks to ensure the implementation of effective controls, appropriate to the organization's risk profile, ensuring compliance with legal and ethical obligations, both nationally and internationally. Contacto assumes the responsibility of promoting an organizational culture based on legality, transparency, and due diligence, acting proactively in facing the threats associated with these crimes.

At Contacto, we acknowledge the importance of preventing our services from being used for illicit purposes. For this reason, we have adopted a zero-tolerance policy on Anti-Money Laundering, Combating the Financing of Terrorism, and the Proliferation of Weapons of Mass Destruction (AML/CFT/WMD).

Contacto is committed to:

- Comply with current regulations in Colombia and applicable international standards.
- Implement an AML/CFT/WMD risk management system proportionate to our nature, structure, and risk profile.
- Promote a culture of legality, integrity, and transparency in all our operations and business relationships.
- Guarantee due diligence in getting to know our customers, collaborators, suppliers, and allies.
- Strengthen mechanisms for detecting, reporting, and preventing suspicious transactions.
- Designate a person responsible for leading the implementation and supervision of this policy.
- Train personnel on a regular basis so as to ensure the understanding and correct application of prevention measures.

2. SCOPE

This policy is mandatory for all collaborators, partners, contractors, and strategic allies involved in the value chain of the services offered by Contacto.

- It applies to all direct and indirect activities, including:
- Management of clients’ financial and operational information.
- Administration of technological platforms.

- Data processing and outsourced services, with no geographical limitation.

Compliance with this policy is an essential requirement for establishing, maintaining, or renewing business relationships with the organization.

3. REGULATORY FRAMEWORK

This policy is based on the applicable international legal provisions and standards on the prevention of AML/CFT/WMD, including, but not limited to:

- Guidelines of the Financial Information and Analysis Unit (UIAF, for its acronym in Spanish).
- Regulations issued by the Superintendence of Companies and other control entities.
- International standards of the Financial Action Task Force (FATF).
- Regulations related to Know Your Customer (KYC) and due diligence.
- Colombian Criminal Code, on matters related to financial crimes.

4. GENERAL PRINCIPLES

- Commitment to legality and business ethics.
- Application of the risk-based approach.
- Confidentiality, integrity, and traceability of the information.
- Regulatory compliance and self-regulation.
- Continuous improvement of the prevention system.

5. ROLES AND RESPONSIBILITIES

- Legal Representative: Guarantees the effective implementation of the policy, allocating the necessary resources for its execution.
- Employees: Apply the policy in their daily duties, reporting unusual or suspicious operations.
- Process Directors and Leaders: Verify operational compliance with this policy and its related procedures, promoting a culture of compliance.

6. PREVENTION MEASURES

- Client identification and knowledge, and due diligence.
- Regular risk assessments, considering the kind of client, economic sector, jurisdiction, and nature of the service.

- Monitoring unusual operations and timely reporting to the UIAF.
- Ongoing and updated training of risk-exposed personnel.
- Minimum documentary conservation of five (5) years, in accordance with the law.

7. DATA PROTECTION AND CONFIDENTIALITY

Information collected and processed within the framework of this policy will be treated pursuant to the principles set forth by Law 1581 of 2012 and its regulatory standards, guaranteeing:

- Exclusive use for the purposes of the prevention system.
- Access restricted to authorized personnel.
- Effective protection of its confidentiality, integrity, and availability.
- Technological and administrative measures will be implemented to prevent leaks, unauthorized access, or improper manipulation.

8. REVIEW AND UPDATE

This policy will be reviewed at least once a year to ensure its effectiveness and alignment with current best practices and regulations. Furthermore, it may be updated whenever:

- Regulatory or policy changes.
- New types of risks or emerging threats are identified.
- Structural or technological modifications that impact critical processes are implemented.
- There are failures, gaps or operational incidents requiring corrective actions.