TECTRIL

ANTI-MONEY LAUNDERING, FRAUD AND SANCTIONS POLICY

Integrity, due diligence and controls in domestic and international operations

CAMPO	INFORMAÇÃO
Company	Tectril Soluções em Logística e Comércio Ltda. (“Tectril”)
Código	02-EN
Revision	0
Data	20/07/2026
Language	English
Status	Institutional draft — subject to internal approval and legal validation before publication

Institutional draft — subject to internal approval and legal validation before publication

1. Purpose

This Policy establishes principles, responsibilities and controls to prevent, identify, assess, stop and internally report situations involving money laundering or concealment of assets, rights and funds, terrorist and proliferation financing, fraud, and breaches of applicable sanctions or trade and financial restrictions.

Tectril does not permit its structure, services, accounts, documents, foreign-trade operations, transportation, warehousing, payments or relationships to be used to disguise illicit proceeds, conceal beneficial owners, defraud controls or circumvent applicable restrictions.

2. Scope

It applies to directors, employees, interns, temporary workers and anyone acting on behalf of Tectril, and, as appropriate, to customers, suppliers, agents, customs brokers, carriers, consultants, partners, representatives and other third parties.

It covers Tectril's own operations and services performed under Tectril's or the customer's RADAR authorization, including imports, exports, IOR/EOR, transportation, warehousing, repair and return, special customs regimes, international payments and records management.

3. Principles

- legality, ethics, good faith, transparency and traceability;
- risk-based approach and proportional controls;
- knowledge of the customer, supplier, partner, beneficial owner and transaction purpose;
- segregation of duties, appropriate approvals and reliable records;
- non-retaliation for good-faith reports;
- lawful cooperation with authorities, while preserving confidentiality and applicable rights.

4. Key definitions

Money laundering

Concealing or disguising the origin, location, movement, ownership or nature of assets, rights or funds derived directly or indirectly from a criminal offense.

Terrorist and proliferation financing

Providing, collecting or moving funds for terrorism or the proliferation of weapons of mass destruction, even when the funds have a lawful origin.

Fraud

An intentional act of deception, falsification, omission, manipulation or abuse of trust to obtain an undue advantage or cause loss.

Beneficial owner

The natural person who ultimately owns, controls or benefits from a legal entity, arrangement or transaction.

PEP

Politically exposed person under applicable legal and regulatory criteria, including related situations requiring enhanced due diligence.

Sanctions

Restrictive measures such as asset freezes, prohibitions on making funds available, embargoes, or trade, financial, territorial or sectoral restrictions.

5. Governance and responsibilities

- Executive Management: approve the Policy, provide resources, and decide on critical risks and exceptions that are not legally prohibited.
- Compliance: maintain the risk methodology; guide due diligence; review alerts; define measures; preserve records; coordinate training; and, with Legal, assess reports to authorities.
- Legal: interpret legal, regulatory, contractual and sanctions requirements and support suspension, rejection, blocking or reporting decisions.
- Finance: validate account ownership, payment consistency, reconciliations and evidence; prevent unauthorized payments.
- Sales and Operations: understand the purpose and participants; verify documents; stop and escalate inconsistencies.
- Everyone: follow controls, never ignore alerts and immediately report concerns through the designated channel.

6. Risk assessment

Tectril will periodically assess risk considering the service, customer, third party, country, route, goods, sector, payment channel, beneficial owner, contracting method, value, frequency, complexity, intermediaries and exposure to PEPs or restricted lists. Risk may be rated low, medium, high or unacceptable.

High risk requires enhanced due diligence, documented rationale and approval from Compliance and, when required, Executive Management. Unacceptable risk or a legal prohibition requires rejection, suspension or termination, with legal advice.

7. Know your customer and third parties (KYC/KYB/KYS)

- identify and validate the legal entity, representatives, ownership chain and beneficial owner;
- confirm business activity, address, reputation, source and purpose of the relationship;
- screen PEPs, sanctions, restricted lists, relevant adverse media and high-risk jurisdictions;
- verify licenses, authorizations, operational capacity and consistency among service, goods, price, route and documents;
- obtain source of funds and/or wealth where justified by risk;
- refresh records periodically and upon material change.

8. Sanctions and restrictions screening

Before onboarding and at relevant transaction stages, the parties, beneficial owners, banks, vessels, aircraft, countries, territories, goods and other relevant elements must be screened.

Sanctions effective in Brazil are mandatory, including those arising from the United Nations Security Council. Other lists, such as U.S. OFAC, European Union and United Kingdom lists, will be observed when legally, territorially or contractually applicable, or as a risk factor. Potential matches must be validated to avoid false positives. Advising on or executing sanctions-evasion structures is prohibited.

9. Fraud prevention and detection

- validate tax, customs, commercial, banking and transport documents for authenticity and consistency;
- segregate request, approval, payment, reconciliation and master-data changes;
- confirm bank-account changes independently with a previously authorized contact;
- prohibit unrelated third-party payments, personal accounts, false documents, over/under-invoicing and misleading descriptions;

- control access, versions, audit trails and evidence;
- investigate conflicts of interest, duplicates, unusual commissions, atypical refunds and diversion of goods or funds.

10. Red flags

- refusal or unjustified delay in disclosing beneficial ownership or source of funds;
- overly complex or inconsistent ownership with no apparent economic purpose;
- cash, cryptoasset or unjustified third-party payment; structuring or unusual urgency;
- payment from/to a country, bank or account unrelated to the transaction;
- inconsistent price, quantity, weight, classification, origin, destination or description;
- altered, conflicting, duplicate or apparently false documents;
- routes, transshipments or intermediaries without commercial justification;
- requests to omit information, change dates, descriptions or values, or evade licenses, taxes, customs controls or sanctions;
- relevant adverse media, undisclosed PEP or possible restricted-list match;
- resistance to controls, pressure to release goods or a promise of improper advantage.

11. Payments and financial controls

- payments and receipts must use an account owned by a party consistent with the contract and be supported by documents;
- exceptions require justification, third-party identification, proof of relationship and prior Finance and Compliance approval;
- secret, fictitious, unsupported, off-book or illicit facilitation payments are prohibited;
- foreign-exchange transactions must use authorized institutions and reflect the true nature of the transaction;
- refunds should preferably return to the originating account;
- approval limits, dual approval and independent reconciliation must be observed.

12. Alert handling and decisions

1. Stop processing, where safe and permitted, if continuing may increase risk.
2. Preserve documents and notify Compliance without tipping off the person involved.
3. Review identity, context, evidence, legal basis, sanctions risk and need for additional diligence.
4. Decide and record whether to clear, impose conditions, enhance monitoring, reject, suspend, terminate, block when legally required, or report to the competent authority.
5. Limit information to those with a need to know and prohibit retaliation.

13. Reporting to Coaf and authorities

Whether Tectril is an obliged entity under Law No. 9,613/1998 depends on the specific classification of its activities. Compliance and Legal must periodically verify this status and the rules of the competent regulator.

Where legally required, a report will be submitted within the required period through the official channel, without notifying the person involved and while preserving confidentiality. Where no specific reporting duty applies, Tectril will assess lawful measures with legal counsel. No employee may report on behalf of the company without authorization, except where personally required by law.

14. Records, privacy and confidentiality

Onboarding files, due diligence, approvals, alerts, analyses, decisions and evidence will be retained for the legal, regulatory, contractual or records-schedule period, whichever applicable period is longer. Records must be reliable, traceable, accessible only to authorized persons and protected from improper alteration or destruction.

Personal data processing will comply with Brazil's LGPD, including purpose limitation, necessity, security, access control and secure disposal. Investigations and reports are confidential.

15. Training, monitoring and audit

Tectril will provide periodic, role-appropriate training. Compliance will monitor control effectiveness, indicators, exceptions and action plans. Independent audits or reviews may test samples, registrations, payments, screening and records. Deficiencies must have an owner and remediation deadline.

16. Violations and disciplinary measures

Violations may lead to disciplinary measures, contract termination, recovery of losses and reporting to authorities, without prejudice to civil, administrative and criminal liability. Commercial targets never justify bypassing controls. Good-faith reporting will be protected; knowingly false allegations may be investigated.

17. Reporting channel

Questions and alerts must be sent to compliance@tectril.com.br or Tectril's Integrity Channel. Urgent situations must be reported immediately. The channel does not replace public emergency services.

18. Effective date, review and approval

This Policy takes effect upon approval. It will be reviewed at least every two years, or earlier following a legal change, material risk change, significant incident or identified deficiency. Exceptions may be approved only when lawful, justified and formally recorded; legal prohibitions allow no exception.

19. Main legal and regulatory references

- Law No. 9,613/1998 — money laundering and prevention
- Law No. 12,846/2013 — corporate liability
- Decree No. 11,129/2022 — Anti-Corruption Law regulation
- Law No. 13,810/2019 — UN Security Council sanctions
- Decree No. 9,825/2019 — UN sanctions regulation
- Coaf — system, rules and FATF notices

The references must be confirmed during final legal review and supplemented according to the sectors, countries, customers, banks, goods and contracts involved.

APPROVAL

Prepared by	Reviewed by	Approved by	Date