TECTRIL | THIRD-PARTY GOVERNANCE

THIRD-PARTY MANAGEMENT AND DUE DILIGENCE POLICY

Integrity and governance guidelines for selecting, engaging, monitoring and exiting third-party relationships

Tectril Soluções em Logística e Comércio Ltda.

Caieiras – SP | 2026

Institutional draft for internal approval and legal validation

Document Control

Field	Information
Code	POL-SUP-001
Language	02-EN | English
Revision	Rev. 0
Status	Draft for approval
Classification	Internal use
Owner	Tectril Management
Management	Person designated for Integrity and Compliance
Approval	Tectril Management
Effective date	Upon formal approval
Review cycle	Annually or upon a relevant change

Related Documents

- Code of Ethics and Business Conduct
- Compliance Policy
- Anti-Corruption Policy
- Code of Conduct for Suppliers, Service Providers and Business Partners
- PRO-SUP-001 — Supplier and Service Provider Engagement, Due Diligence and Management Procedure
- PRO-CPL-001 — Conflicts of Interest, Gifts, Meals, Hospitality and Travel Procedure
- Privacy, Information Security and Records Management Policies, as applicable

Table of Contents

1. Purpose

To establish Tectril's principles and guidelines for managing relationships with suppliers, service providers, consultants, representatives, intermediaries, partners, subcontractors and other third parties in proportion to risk.

This Policy aims to ensure legitimate business need, responsible selection, technical and financial capability, integrity, legal compliance, reasonable compensation, appropriate approvals, documentation and monitoring throughout the relationship lifecycle.

2. Scope

This Policy applies to directors, employees, workers and any person who requests, assesses, approves, engages, registers, pays or monitors third parties on Tectril's behalf, in Brazil or abroad.

It covers purchases and engagements of any kind, including professional services, technology, facilities, logistics, transportation, warehousing, customs brokers, freight forwarders, consultants, representatives, materials, regulated services and operating partnerships. The depth of controls shall be proportionate to risk.

3. Principles

- Legality, ethics, integrity, good faith and respect for human rights.
- Genuine need, legitimate business purpose and no improper favoritism.
- Objective selection based on capability, quality, integrity, risk, total cost and documented terms.
- Due diligence before commencement and risk-based monitoring throughout the relationship.
- Segregation of duties and independent review whenever practicable.
- Transparency regarding ownership, ultimate beneficial owners, conflicts, commissions, intermediaries and subcontracting.
- Payment only for evidenced goods or services, supported by valid documentation and an account consistent with the contracting party.
- Data protection, confidentiality, information security and preservation of evidence.
- The right and duty to stop the process when information is incomplete, inconsistent or irregular.

4. Selection and engagement guidelines

Every engagement must arise from a defined need, clear scope, compatible budget and identified internal owner. Selection must consider total price, quality, timing, capability, integrity, continuity, risks and commercial terms.

As a governance rule, comparable proposals should be sought where market conditions and proportionality allow. Lowest price does not automatically determine the choice. Sole source, genuine emergency, technical continuity, exclusivity, standardization or lack of market requires documented justification and approval; poor planning is not an emergency.

- Actual, potential or apparent conflicts of interest must be disclosed and addressed before a decision.
- No third party may start work before applicable checks, approvals, contractual instrument and registration are complete, except under a formal exception.
- Only persons with current authority may undertake obligations or sign on Tectril's behalf.

5. Due diligence and risk classification

Third-party due diligence (3PDD) assesses, as appropriate to risk, identity and registration, ownership and ultimate beneficial ownership, capability, experience, licenses, relevant financial and tax status, sanctions, politically exposed persons (PEPs), government links, reputation, proceedings, conflicts, commissions, subcontractors and integrity controls.

Compliance records the classification as low, medium, high or unacceptable and may raise it according to country, activity, access, value, criticality or red flags. Any reduction requires documented justification. Only data that are adequate, necessary and relevant to the purpose may be collected.

Indicative risk matrix

Level	Typical characteristics	Minimum response
Low	Occasional purchase or simple service, with no relevant access, representation, government contact or regulated activity.	Registration and identity, conflict check, scope/price, bank account, approval and evidence of delivery.
Medium	Recurring service, dependency, limited access, subcontracting, material impact or international activity.	Questionnaire, beneficial ownership, licenses, sanctions, reputation, proportionate financial review, contract and monitoring.
High	Representation, public official, critical customs/logistics, data or funds, commission, PEP, high-risk jurisdiction or material red flag.	Enhanced 3PDD, legal review, additional clauses and controls, Management approval and periodic reassessment.

6. Red flags and decisions

Red flags include, among others: refusal or unjustified delay in providing information; hidden owner or beneficiary; inadequate capability; government connection; unusual referral by a decision-maker; excessive commission; cash payment, payment to a third party, personal account or unrelated country; inconsistent documents; relevant adverse media; sanctions; missing license; abnormal price; artificial urgency; improper secrecy request; resistance to integrity clauses; undisclosed subcontracting; or premature commencement.

When a red flag arises, the affected stage must stop pending clarification. Compliance may approve with controls, expand diligence, request legal review, impose conditions, suspend, replace or reject the third party. An unresolved material red flag prevents engagement or continuation. Unacceptable risk may not be approved.

7. Contractual requirements and commencement

The instrument must be proportionate to the subject matter and risk and, where applicable, address parties and authority; scope, deliverables, acceptance, term and service levels; price, taxes, currency, expenses and payment; confidentiality, data, security and intellectual property; integrity, anti-corruption, sanctions and conflicts; subcontracting; audit; licenses, insurance, health, safety and environment; incidents, continuity, amendment, suspension, termination and return of assets or data.

Medium- and high-risk third parties must have a written contract and accept the applicable Code of Conduct, unless an exception is approved. Before commencement, Tectril must complete approvals, validate registration and bank details through an independent channel, brief the third party and appoint the monitoring owner.

8. Payments and financial records

- Payments must match the approved contract, purchase order or instrument, evidenced delivery, valid tax documentation and a truthful description.
- The payee, bank account and payment country must be consistent with the contracted third party and the transaction; changes to bank details require independent confirmation.
- Improper, unsupported, duplicate or split payments intended to evade approval limits, incompatible cash payments, and payments to unapproved third parties are prohibited.
- Finance must stop payment when there is a material inconsistency and involve the owner and Compliance when a red flag exists.

9. Monitoring, changes and renewal

Performance and risk must be monitored throughout the relationship, considering quality, timing, incidents, complaints, licenses, contract status, payments, red flags and remediation plans. Higher-risk or critical third parties require more frequent oversight.

Material changes in ownership, control, scope, country, bank account, subcontractor, license, sanctions, investigation, incident, financial condition or method of operation must be reported and assessed before continuation. Renewal is not automatic and requires review of need, performance, price, risk, documents, conflicts, term and approvals.

10. Subcontracting and third-party chain

A third party may not subcontract material activities or transfer obligations without authorization where required by the contract or risk. Tectril may require identification, due diligence and controls for subcontractors, agents, intermediaries and other members of the chain.

Authorization to subcontract does not relieve the principal third party of responsibility for complying with law, contract and Tectril standards.

11. Data protection, confidentiality and security

Information and personal data must be processed for a legitimate purpose, with restricted access, security measures and retention consistent with law, contract and Tectril policies. The third party must report incidents and cooperate with investigation, containment, remediation and responses to data subjects or authorities where applicable.

Access to systems, premises, documents, assets or data must follow need-to-know, least-privilege and timely revocation principles. Information obtained through due diligence is confidential and available only to those who need it.

12. Exit from the relationship

At exit, deliveries and payments must be confirmed, access and powers revoked, assets recovered, data returned or deleted as applicable, warranties and disputes addressed, registration updated and the file preserved.

An integrity-related termination must be coordinated with Compliance, Management and legal counsel where needed, while preserving evidence, rights and safe continuity.

13. Responsibilities

Management

- Approve the Policy and designate owners; provide resources and segregation or compensating controls; approve engagements, exceptions and risks within authority; confirm signing powers; decide critical matters without participating when conflicted.

Requestor and service owner

- Justify the need, define scope and criteria, assess capability, oversee delivery and performance, record acceptance, and report changes, incidents and red flags.

Finance

- Check budget, price, taxes, registration, relevant financial condition, invoicing, bank details and payment consistency; block unsupported or inconsistent payments.

Integrity and Compliance

- Classify risks, coordinate 3PDD, assess sanctions, PEPs, reputation, conflicts and red flags, define controls, record decisions and monitor relevant third parties.

Legal counsel

- When engaged, review contracts, authority, liability, data, intellectual property, regulatory matters, governing law, termination and other legal risks.

Third party

- Provide true and current information; disclose owners, beneficiaries, conflicts and subcontractors; maintain licenses; comply with law, contract and Tectril Codes; keep records and report changes.

14. Records and retention

Tectril must maintain a risk-proportionate electronic file containing the request, proposals, justifications, selection, exceptions, questionnaires, checks, 3PDD report, approvals, contract and amendments, registration, delivery and payment evidence, monitoring, renewal and exit.

Records must be complete, traceable, protected and retained for at least five years after exit, or longer where required by law, contract, retention schedule, investigation, audit or dispute. Disposal must be secure and suspended when a preservation duty applies.

15. Reporting, non-retaliation and consequences

Questions, concerns or suspicions must be reported to compliance@tectril.com.br or through the Integrity Channel. Retaliation against anyone who in good faith stops, questions, refuses or reports a situation is prohibited.

Violations may result in process suspension, additional controls, payment refusal, blocking, termination, disciplinary action, recovery of losses, reporting to authorities and other appropriate measures, subject to proper review.

16. Exceptions, effectiveness and review

Administrative exceptions must be approved in advance, justified, temporary, documented and approved by Management; integrity or high-risk matters require a Compliance opinion. No exception may authorize corruption, fraud, concealed conflicts, false records, unauthorized signatures, payment without delivery or any unlawful act.

This Policy becomes effective upon formal approval and must be reviewed annually or whenever there is a relevant change in law, structure, authority, systems, risk profile or Tectril operations. If requirements conflict, applicable law and valid contractual instruments prevail, without limiting stricter controls.

Note: this document is an institutional draft and must undergo internal approval and legal validation before becoming effective.