

TECTRIL

INTEGRITY REPORTING CHANNEL POLICY

Receipt, protection, investigation and responsible handling of reports

CORE COMMITMENT. Every report will be received respectfully, handled on a need-to-know basis and assessed impartially. Tectril will not tolerate retaliation against anyone who acts in good faith.

Document	Version	Effective date
Integrity Reporting Channel Policy	Revision 0	July 18, 2026

TECTRIL SOLUÇÕES EM LOGÍSTICA E COMÉRCIO LTDA
Caieiras — São Paulo — Brazil

Document control

Field	Definition
Owner	Tectril Management
Operational management	Formally appointed Integrity Reporting Channel Officer
Approval	Tectril Management
Review cycle	Annually, or whenever a relevant process, organizational or legal change occurs
Classification	Public institutional document
Related documents	Code of Business Ethics and Conduct; Integrity Reporting Channel Privacy Notice; Records Management Policy; Information Security Policy

1. Purpose

This Policy establishes the rules for receiving, recording, screening, preliminarily assessing, investigating, deciding, closing and retaining reports submitted to Tectril's Integrity Reporting Channel. Its purpose is to ensure an accessible, reliable, confidential, impartial and documented process consistent with personal data protection requirements.

It also establishes safeguards against retaliation and independence mechanisms for matters involving shareholders, directors, senior leaders or the person responsible for managing the Channel.

2. Scope

This Policy applies to reports submitted by employees, applicants, former employees, clients, suppliers, service providers, partners, representatives, public officials and any other persons who have or have had a relationship with Tectril.

It covers facts connected with Tectril's activities in Brazil or abroad, including conduct by third parties acting in Tectril's name or interest.

3. Channel principles

- Good faith: the reporting person does not need certainty that misconduct occurred, but must report sincerely and provide information reasonably available to them.
- Confidentiality: the identity of the reporting person and report information will only be accessed by persons who need the information to handle the case.
- Option not to identify oneself: the dedicated form may be used without requiring a name, email address or telephone number.
- Impartiality: decisions will be based on facts, records and objective criteria, with fair consideration of the persons involved.
- Independence: no person may receive, investigate or decide a matter in which they have personal interest, direct hierarchical involvement or participation in the reported facts.
- Non-retaliation: retaliation against anyone who reports or cooperates in good faith is prohibited.

- Necessity and proportionality: only information appropriate and necessary for handling the report will be collected and used.
- Traceability: relevant steps and decisions will be securely documented, preserving the chain of custody of evidence.

4. Reporting channels and reporting options

4.1. Integrity Reporting Channel form

The form made available on Tectril's official website is the recommended reporting method. Before completing it, the person must choose one of the following options:

Option	Operation
Identified and confidential	The person voluntarily provides contact details. Their identity remains restricted to authorized persons and will only be shared when necessary, in a limited manner, or when legally required.
Without identification	Name, email and telephone are not required. The person should avoid including information in the narrative or attachments that reveals their identity. Lack of contact information may prevent requests for clarification and communication of the outcome.

4.2. Channel email

The address canaldeetica@tectril.com.br is intended for identified and confidential reports, questions and requests for guidance. Email will not be presented as an anonymous method because the sender's address and other technical data may permit identification.

4.3. Reports made to a leader or other representative

Anyone who receives a report in a conversation, message or through another method must promptly, discreetly and accurately forward it to the Channel Officer. They must not conduct an independent investigation, promise a result or share the content with unauthorized persons.

5. Matters that may be reported

The Channel may be used for suspected or actual:

- fraud, corruption, bribery, improper favoritism or conflicts of interest;
- moral or sexual harassment, discrimination, violence or threats;
- tax, customs, regulatory, accounting or documentary misconduct;
- violations of sanctions, embargoes, export controls or international trade rules;
- misuse of information, personal data, assets, resources or intellectual property;
- falsification, concealment, destruction or manipulation of records or evidence;
- violations of the Code of Ethics, internal policies, contracts or applicable law;
- retaliation, attempts to prevent reporting or interference with an investigation.

NOT AN EMERGENCY CHANNEL. Situations involving immediate risk to life, physical integrity or safety must be reported to the competent public emergency services. The Channel does not replace commercial support, operational assistance or routine complaints that do not involve an ethics concern.

6. Governance and responsibilities

Role	Core responsibilities
Tectril Management	Approve the Policy; formally appoint the Channel Officer and alternate; provide resources; decide high-impact measures; review aggregated indicators without unnecessary disclosure of identities.
Channel Officer	Receive, record and screen reports; protect information; assess conflicts; coordinate investigations; maintain records; communicate decisions; monitor retaliation and report aggregate results.
Formally appointed alternate	Take over when the primary Officer is absent, conflicted or otherwise disqualified.
Internal or external investigator	Conduct authorized inquiries, preserve evidence, record objective conclusions and maintain confidentiality.
Decision-making management	Assess conclusions and determine corrective, disciplinary or remediation measures without replacing the technical investigation.
All covered persons	Cooperate in good faith, preserve records, maintain confidentiality and refrain from retaliation.

7. Independence, conflicts and sensitive reports

An appointed person must recuse themselves whenever they are involved in the facts, have a relevant personal relationship, direct reporting line, financial interest, participation in a challenged decision, or any other circumstance that may compromise or appear to compromise impartiality.

7.1. Mandatory routing

Person implicated	Mandatory routing
Channel Officer	The formally appointed alternate handles the matter without access by the conflicted Officer.
Channel alternate	The primary Officer handles the matter, provided the Officer is not conflicted.
Shareholder, director or senior leader	The matter is referred directly to an independent external professional or adviser engaged to assess the report, preserve evidence and recommend measures.
All internal responsible persons potentially implicated	Tectril uses an independent external party with segregated access and reporting to a non-implicated person or corporate body.

An implicated person may not access the record, select the investigator, restrict inquiries, participate in the decision or receive information that could identify the reporting person, except where legally required or strictly and demonstrably necessary.

8. Handling process

1. Receipt and registration. The report is recorded in a restricted-access environment with the date, channel, reporting option and original description. Original content is not altered; summaries are identified as such.
2. Acknowledgment. Where secure contact is available, Tectril acknowledges receipt within two business days. For a free form without contact information or a trackable case number, acknowledgment is displayed on screen after submission.
3. Screening. Within ten business days, the Channel assesses scope, urgency, risks to persons, risk of evidence destruction, conflicts of interest, immediate preservation needs and initial sufficiency of information.
4. Preliminary assessment. Plausibility, available sources and any necessary interim measures are reviewed. Lack of complete initial evidence does not automatically justify dismissal.
5. Investigation plan. Where appropriate, scope, investigator, inquiries, documents, interviews, access controls and an estimated timeline are defined.
6. Investigation. The inquiry may include document review, interviews, systems validation and other lawful, proportionate procedures. Persons involved have an appropriate opportunity to provide information without improper access to the reporting person's identity.
7. Conclusion and decision. The closing report distinguishes substantiated, unsubstantiated and inconclusive matters, identifies evidence and recommends measures. A competent, non-conflicted authority decides the outcome.
8. Closure and monitoring. The record is closed after the decision and action plan. Where possible, a general notice is provided to the reporting person, subject to confidentiality, third-party rights and legal limits. Retaliation risk and corrective action may continue to be monitored.

8.1. Target completion time

Tectril will seek to complete an investigation within 60 calendar days after screening. Complex matters may require additional time, which must be justified and documented. This target does not limit immediate protective or preservation measures.

9. Additional information and communications

Where contact is available, the Channel Officer may request clarifications, documents or witness information. The reporting person may voluntarily supplement the report while it remains under review.

Reports without identification and without a tracking function may not permit follow-up or response. This limitation must be clearly disclosed before submission.

Where possible, closure communications will be general and will not disclose individual disciplinary action, third-party personal data, legal strategy, confidential documents or information that could prejudice an investigation.

10. Preservation of records and evidence

Upon receipt, Tectril may issue preservation instructions to prevent alteration, deletion or loss of related physical and digital records. The process must:

- preserve the original report and record all supplements;
- document the source, collection date, custodian and relevant movement of evidence;
- preserve relevant emails, messages, documents, system records, images and other materials;
- suspend routine destruction where there is an investigation, dispute, audit, inspection or preservation duty;
- avoid excessive collection or indiscriminate access to personal accounts, devices and files;
- document interim and preservation decisions.

Destroying, altering, concealing or directing the alteration of evidence, or retaliating against someone for preserving or presenting evidence, is prohibited.

11. Personal data protection and security

Personal data is processed to receive, assess, investigate and remediate possible misconduct, protect rights, comply with legal or regulatory obligations and exercise rights in administrative, arbitral or judicial proceedings, according to the legal basis applicable to each activity.

Where a report contains sensitive personal data, processing will be limited to what is strictly necessary and subject to enhanced safeguards under applicable law and internal rules.

- need-to-know access and individual permissions;
- secure authentication and periodic access review;
- logging of relevant access and operations where technically available;
- protected transmission and storage;
- minimum necessary sharing with investigators, advisers or competent authorities;
- confidentiality instructions for investigation participants;
- secure deletion or anonymization after the retention period where no basis for continued retention exists.

TRANSPARENCY. The form must display a dedicated Privacy Notice explaining purposes, data categories, sharing, data subject rights, retention and the contact channel for data protection matters.

12. Retention and disposal

Channel records will be retained for as long as necessary for investigation, remediation, demonstration of the Integrity Program, exercise of rights and compliance with applicable obligations.

As an initial internal rule, the case file will be retained for five years after closure, subject to periodic necessity review. The period may be extended for legal or contractual obligations, an ongoing investigation, preservation measure, judicial, administrative or arbitral proceedings, audit, inspection or documented legal risk.

After the period expires and no basis for continued retention remains, data will be securely deleted or anonymized. Backups will follow Tectril's protected technical replacement cycle.

13. Non-retaliation and protective measures

Tectril prohibits retaliation against anyone who in good faith reports, raises a concern, refuses potentially improper conduct, participates in an interview, preserves records or cooperates in an investigation. Retaliation may include:

- dismissal, threats, punishment, exclusion, humiliation or unfair assessment;
- unjustified harmful changes to duties, hours, compensation, opportunities or working conditions;
- termination, restriction or commercial threats motivated by the report;
- attempts to discover an unidentified reporting person's identity without legitimate need;
- pressure to withdraw, change or withhold a report;
- hostility toward witnesses, investigators or persons preserving evidence.

Suspected retaliation will receive priority and may lead to protective, corrective, contractual or disciplinary measures. Protection does not prevent consequences for the reporting person's own proven misconduct, provided those consequences are not motivated by the report.

14. Unsubstantiated reports, mistakes and bad faith

14.1. Unsubstantiated or inconclusive report

A good-faith report does not become false merely because an investigation finds insufficient evidence or concludes that no violation occurred. The matter will be classified as unsubstantiated or inconclusive, without penalty to the reporting person.

14.2. Deliberately false report

Bad faith means knowingly submitting false information, fabricating evidence or intentionally using the Channel to harm another person. Bad faith must be established through objective evidence and may not be presumed merely because a report was not substantiated. If proven, proportionate measures may be taken following impartial review and applicable legal, contractual and internal rules.

15. Measures following an investigation

Depending on the nature and seriousness of the matter, Tectril may provide guidance or training, improve controls, correct records, revise processes, strengthen contractual provisions, adopt interim removal, impose disciplinary action, terminate a contract, recover losses or notify competent authorities.

Measures must be proportionate, documented, consistent and decided by a non-conflicted person. Interim measures do not constitute a premature finding of responsibility.

16. Indicators and accountability

The Channel Officer will periodically provide Management with aggregated information on report volumes, categories, timeframes, status, remediation and retaliation indicators. Management reports must avoid unnecessary identification of reporting persons, witnesses or involved persons.

Management will assess Channel effectiveness, process independence, access security, compliance with timelines and implementation of corrective actions.

17. Training and communication

Tectril will communicate the Channel and this Policy to relevant audiences, explaining reporting options, non-retaliation, confidentiality duties and the limits of anonymity. Persons receiving or investigating reports will receive specific guidance on impartiality, data protection, interviews, evidence preservation and decision records.

18. Violations of this Policy

Violations include unauthorized access to a report, improper disclosure of identity or content, failure to disclose a conflict, interference with an investigation, destruction of evidence, retaliation, failure to forward a received report or violation of a formal preservation instruction. Violations will be impartially assessed and may result in appropriate disciplinary, contractual and legal measures.

19. Final provisions

This Policy takes effect upon approval and must be interpreted together with Tectril's Code of Business Ethics and Conduct and other policies. Applicable law and the rule that best preserves investigation integrity and the rights of involved persons will prevail in the event of conflict.

The Policy will be reviewed at least annually, or earlier following relevant changes to the Channel, organizational structure, identified risks or legislation.

20. Approval

Responsibility	Name/Position	Date	Signature
Preparation			
Legal/data protection review			
Approval			

Appendix I — Minimum report information

The form should allow proportionate and accessible submission of:

- reporting option: identified and confidential, or without identification;
- report category;
- relationship with Tectril, with an option not to disclose;
- clear description of events;
- persons, companies, functions or locations involved;
- approximate date or period;
- immediate risk, continuing conduct or retaliation risk;
- witnesses or information sources;
- documents and attachments, with a warning about metadata that may identify the reporting person;
- declaration that the information is submitted in good faith.

Appendix II — Outcome classification

Classification	Meaning
Substantiated	Evidence sufficiently supports the occurrence of the fact or violation.
Partially substantiated	A relevant part is supported, while other elements are not established.
Unsubstantiated	Available evidence indicates that the fact did not occur or was not a violation.
Inconclusive	Sufficient evidence could not be obtained to confirm or rule out the report.
Outside scope	The matter does not belong in the Channel and is referred appropriately, with the referral documented.
Proven bad faith	Objective evidence shows knowing fabrication of information or evidence with intent to harm.

Legal and good-practice references

- BRAZIL. Law No. 12,846/2013 — Brazilian Anti-Corruption Law.
- BRAZIL. Decree No. 11,129/2022 — regulates Law No. 12,846/2013 and addresses integrity programs.
- BRAZIL. Law No. 13,709/2018 — Brazilian General Data Protection Law (LGPD), as amended.
- OFFICE OF THE COMPTROLLER GENERAL OF BRAZIL (CGU). Integrity Program: Guidelines for Private Companies, Volume II, 2024.
- ABNT NBR ISO 37002 — Whistleblowing management systems — Guidelines, as a good-practice reference where applicable.

VALIDATION NOTE. This version establishes an initial governance framework and should be reviewed by legal and data protection professionals before formal approval, particularly regarding legal bases, retention, employment matters and technical form configuration.