

TECTRIL

Integrity Channel

Canal de Integridade | Canal de Integridad

ENGLISH

TRILINGUAL DOCUMENT Institutional information for employees, officers, suppliers, customers, business partners and other stakeholders.

This content has been prepared for publication following the technical and operational validation of the Integrity Channel. This document does not replace specific legal advice.

ENGLISH

Tectril Integrity Channel

Responsible listening, impartial handling, and protection against retaliation.

EN Tectril Soluções em Logística e Comércio Ltda. | Revision 0 | July 19, 2026

1. What the Integrity Channel is

The Tectril Integrity Channel is a secure and responsible means for reporting conduct that may violate applicable law, the Code of Conduct, internal policies, the company's ethical commitments, or individual rights. It is part of Tectril's Integrity Program and is available to employees, officers, candidates, suppliers, service providers, customers, partners, and other stakeholders.

PURPOSE To enable legitimate concerns to be raised in good faith, assessed independently, and handled in a proportionate, documented, and respectful manner.

2. Matters that May be Reported

- corruption, bribery, fraud, conflicts of interest, or improper favoritism;
- workplace bullying, sexual harassment, discrimination, violence, or human-rights violations;
- retaliation against anyone who reports a concern, assists an investigation, or refuses misconduct;
- theft, misappropriation, falsification, or misuse of assets, data, or resources;
- violations of customs, tax, labor, environmental, competition, foreign-trade, or sanctions rules;
- irregularities involving imports, exports, transportation, tariff classification, documents, records, payments, or internal controls;
- breaches of privacy, data protection, confidentiality, information security, or intellectual property;
- serious health, safety, environmental, or physical-integrity risks;
- breaches of Tectril's Code of Conduct, internal policies, contracts, or ethical standards;
- concealment, destruction, or manipulation of evidence.

Routine customer-service, billing, commercial, or human-resources requests should normally be directed to the responsible business channel. The Integrity Channel may be used when the matter involves suspected misconduct or a risk of retaliation.

3. How to Submit a Report

Once the system is officially launched, reports should be submitted at integridade.tectril.com.br. Describe what happened, when, where and how; identify relevant people, areas, companies or transactions when known; state whether the situation is ongoing or urgent; and attach lawfully obtained evidence. Avoid unnecessary personal or sensitive data. Keep the tracking number and password secure.

You do not need proof that a violation occurred. A good-faith report of facts or indications that reasonably warrant review is sufficient.

4. Identification and Anonymity

The channel should accept identified reports and, when technically enabled, anonymous reports. Identification can support follow-up questions. A reporter's identity will be shared only when necessary to handle the matter, subject to legal and procedural limitations. Good-faith reporters will not be penalized merely because a concern is ultimately unsubstantiated.

5. Confidentiality and Personal Data

Information will be restricted on a need-to-know basis and retained for as long as needed for the channel's purposes and applicable legal obligations. Personal data may be processed to receive, triage, investigate, respond to, and document reports; protect rights; comply with legal duties; and establish, exercise, or defend legal claims. Processing will follow applicable law, including Brazil's General Data Protection Law (LGPD), and Tectril's Privacy Policy.

Do not submit third-party personal data, trade secrets, or unrelated documents. Privacy and data-protection requests may be sent to privacidade@tectril.com.br.

6. Protection Against Retaliation

Tectril does not tolerate retaliation against anyone who, in good faith, raises a concern, seeks guidance, assists an investigation, or refuses conduct reasonably believed to be improper. Suspected retaliation should be reported immediately through the Integrity Channel. This protection does not prevent legitimate action based on proven misconduct that is independent of the report.

7. How Reports are Handled

1. Receipt and issuance of a tracking number.
2. Initial triage for subject matter, urgency, conflicts of interest, and immediate protective action.
3. Assignment to an independent, appropriately authorized reviewer or investigator.
4. Collection and preservation of relevant information, with fair treatment of the persons involved.
5. Evidence-based conclusion and recommendations for corrective, disciplinary, preventive, or improvement measures.
6. Closure record and appropriate feedback to the reporter, subject to confidentiality, privacy, and third-party rights.

Tectril may request further information through the secure follow-up area. Timing will depend on complexity and risk. The channel cannot promise a particular outcome, penalty, or full disclosure of an investigation.

8. Investigation Principles

- impartiality and conflict-of-interest management;
- good-faith assessment and respect for every person's dignity;
- confidentiality and need-to-know access;
- proportionality of measures to risks and evidence;
- record preservation and decision traceability;
- no obstruction, evidence destruction, or retaliation;
- referral to competent authorities when required.

9. Responsible Use

Knowingly false reports, fabricated evidence, malicious accusations, or abusive use may lead to appropriate measures. Honest mistakes, unconfirmed perceptions, and inconclusive reports do not constitute bad faith.

For an immediate threat to life, physical safety, or public security, contact local emergency services first and notify Tectril when it is safe to do so.

10. Contacts and Availability

Integrity Channel: integridade.tectril.com.br — subject to completion of implementation and acceptance testing.

Compliance guidance: compliance@tectril.com.br

Privacy and data protection: privacidade@tectril.com.br

IMPLEMENTATION NOTICE Before publication, Tectril must confirm secure storage, tracking number and password, attachments, restricted administrative access, and the follow-up workflow described above.

Governance and Publication Notes

This content was developed as institutional information for the Integrity Channel. It should be reviewed together with Tectril's Code of Conduct, Anti-Corruption Policy, Compliance Policy, Privacy/LGPD Policy, internal investigation procedure, and records-retention schedule.

Normative References

- **Law No. 12,846/2013** — Brazilian Anti-Corruption Law.
- **Decree No. 11,129/2022** — Regulation of the Brazilian Anti-Corruption Law and integrity program requirements.
- **Law No. 13,709/2018** — Brazilian General Data Protection Law (LGPD).
- **Law No. 14,457/2022** — Measures for the prevention and combat of workplace harassment and other forms of workplace violence, where applicable.
- **Other applicable labor, civil, criminal, tax, customs and regulatory laws and regulations**, as relevant to each specific case.

IMPORTANT This document must undergo **legal and technical review and approval** before its final publication.

The records retention policy, access profiles, internal response timeframes and escalation criteria must accurately reflect the Integrity Channel system effectively implemented by the organization.