1 OBJECTIVE

Oi S.A. and its subsidiaries ("Oi" or the "Company") are committed to maintaining the highest ethical and legal standards and to conducting Oi's activities in accordance with all laws, including, but not limited to, Anti-Money Laundering, Terrorist Financing, Sanctions and Export Control Laws (collectively, the "Compliance Laws").

This policy (the "Policy") contains guidelines, standards, and procedures intended to ensure that Oi, Oi Personnel, and Third Parties understand and comply with the Compliance Laws.

The Company will not tolerate any business practice that does not comply with the Compliance Laws or this Policy.

Violations of the Compliance Laws, may expose Oi and Oi Personnel to potential civil and criminal monetary penalties and other non-monetary civil and criminal implications. Oi may also impose penalties on Oi Personnel who violate any Compliance Laws or this Policy.

Oi's Compliance Team will review this Policy at least bi-annually to ensure that it is up to date and designed to promote, achieve and ensure compliance with Compliance Laws.

Oi Senior Management has reviewed and approved the Company's Policy. Oi Senior Management has also taken, and will continue to take, steps to ensure that the Company's Compliance Team receives adequate resources (including in the form of human capital, expertise, information technology, and other resources, as appropriate) that are relative to the organization's breadth of operations, target and secondary markets, and other factors affecting its overall risk profile.

2 TARGET AUDIENCE

The purpose of this Policy is to establish guidelines and mechanisms to prevent and combat Terrorist Financing and outline the procedures and actions that are required to ensure that the Company complies with Sanctions and Export Control Laws and Anti-Money Laundering Laws.

This Policy applies to all business and transactions entered into by Oi, both in Brazil and outside of Brazil. Specifically, the Policy applies to Oi, Oi Personnel, and any Third Party acting on Oi's behalf.

As further detailed below, current Oi Personnel will be provided with a copy of this Policy following its promulgation, and new Oi Personnel will be provided with a copy before on-boarding/the start of Oi's engagement with them, and as appropriate after that. Oi's Policy must be communicated to, and a copy of this Policy must be shared with, Third Parties on a risk-based approach at the outset of our business relationship with them, and as appropriate after that.

To the extent appropriate based on a risk-based approach to a particular transaction, all Oi Personnel must be certain, prior to the transaction, that the transaction is lawful under Compliance Laws and any other applicable laws and regulations.

3 GUIDELINES

3.1 MONEY LAUNDERING AND TERRORIST FINANCING

Money laundering is characterized by commercial or financial operations that seek to incorporate resources of illicit origin, occurring through transactions that aim to eliminate or make it difficult to trace the illegal origin of such resources. According to Brazilian law, this practice is characterized as a crime classified by Law No. 9613, of 1998 (Money Laundering Law).

Terrorist Financing occurs when terrorist organizations and/or countries that host these organizations benefit from the allocation of resources that can be used in the planning, preparation or practice of terrorism. To mitigate such risks, lists of sanctions are established, which are characterized as measures imposed by governments and international organizations to restrict negotiations with countries, entities and individuals that are linked to Money Laundering, terrorism and human rights violations.

3.2 INTERNATIONAL SANCTIONS

Sanctions are measures imposed by governments and international organizations that restrict negotiations, business or activities with certain countries or persons (entities and individuals). They can be exercised in a variety of ways, including:

- Prohibitions on trading with certain countries, individuals or entities;
- Prohibitions on providing goods and services to certain individuals or entities;
- Trade restrictions, including arms embargoes and export bans on certain equipment; or
- Financial restrictions, such as asset freezes and bans on financial transactions.

(a) <u>US Sanctions</u>

In the United States, Sanctions are generally administered and enforced by the US Department of the Treasury's Office of Foreign Assets Control ("OFAC"). US Sanctions generally apply to "US persons," which is defined to include US citizens, US permanent residents (e.g., green card holders), entities organized under US laws (including US financial institutions and in some instances, their non-US branches), and persons (individuals and entities) in the US (including US branches of non-US companies). In some Sanctions programs, Sanctions prohibitions also extend to "persons subject to US jurisdiction," which includes non-US entities owned or controlled by US persons. US persons, wherever they are located, must comply with US Sanctions laws and are generally prohibited from aiding non-US persons and entities engaging in transactions or dealings that would be prohibited if engaged in by a US person.

Non-US persons Oi and Oi Personnel must comply with US Sanctions. For instance, non-US persons, like Oi or Oi Personnel may be subject to US jurisdiction if they "cause" a US person to violate US Sanctions. Furthermore, non-US persons, like Oi or Oi Personnel, can violate US Sanctions regulations and face civil and criminal liability when their transactions directly or indirectly (i) are prohibited as to US persons, **and** (ii) have a direct or indirect connection to a US person or the United States ("US nexus").

A US nexus can include, for example, any financial transaction that transits through a US correspondent bank (including correspondent accounts of US branches of non-US banks); transactions involving, directly or indirectly, "US persons" (individuals or entities), which include US citizens and green card holders, wherever located, all persons within the United States, US companies, and US affiliates (including a US parent, sister company, or subsidiary) or US branches of a non-US company.

For example, Oi Personnel may violate Sanctions if Oi Personnel were to provide or accept funds in USD involving an individual on OFAC's SDN List, as such USD funds likely would transit a US bank and thus involve US persons in a prohibited transaction involving an SDN.

Even in instances where there is no clear US nexus, non-US persons, such as Oi and Oi Personnel, still may face additional risks, including being added themselves to a Restricted Parties List ("designation risk") or other "secondary sanctions" measures if they provide material support to, or partake in specific activities with a blocked person, or engage in other "sanctionable" activities as set forth in certain US Executive Orders and Sanctions statutes.

(b) European Union ("EU") Sanctions

EU Sanctions target various activities involving certain third countries. EU Sanctions programs do not prohibit all business with a Sanctioned Country but involve various types of measures such as investment and financing bans, trade restrictions on specified items (and related services/assistance), and asset freeze restrictions on designated individuals or entities. They also involve Sanctions imposed on certain activities involving particular industry sectors, including the financial, energy, and of importance to Oi, the telecommunications sector ("Sectoral Sanctions"), which may include export bans on a wide range of goods and related services. For example, EU Sanctions on Syria, Iran, Myanmar, Venezuela and Belarus have included restrictions on the provision of telecom and internet monitoring and interception services, while EU Sanctions on Russia, North Korea and Iran have included imposed restrictions on dual-use items.

(c) United Kingdom ("UK") Sanctions

The UK maintains its own Sanctions programs that target various activities involving specified third countries. They are similar to EU Sanctions with respect to the types of Sanctions measures, but there could be important differences between EU and UK Sanctions in relation to relevant concepts and principles, asset freeze designations, and scope of measures.

Both, the Sanctions targets and the nature of the restrictions imposed by the Sanctions are subject to change regularly. Accordingly, the Compliance Team periodically monitors Compliance Laws and Restricted Party Lists.

Oi and Oi Personnel, must comply with all Sanctions, including with respect to the services provided to the Iranian, Syrian, Cuban and Venezuelan embassies, and shall not take any actions that would result in a violation of Sanctions or its contractual obligations relating to Sanctions.

3.3 US EXPORT CONTROLS

The US Export Administration Regulations (EAR) governs the export, re-export, and in-country transfer of certain US commodities, software and technology that are considered subject to the EAR. An item is considered subject to the EAR if it is US origin, located in the United States, contains greater than *de minimis* US-origin controlled content, or is the foreign-produced direct product of certain US software or technology. Oi Personnel shall not transfer any US-origin product, technology, or non-US-origin product with U.S-origin components or technology to outside the United States in violation of Export Control Laws.

All employees who seek to export, reexport or transfer US-origin products, software, technology, know-how, technical data, or other information, must first contact the Compliance Team for assistance in determining whether the export complies with the EAR.

Prior to transferring any US-origin products or technology (e.g., computers, modems, routers, software or certain data), or non-US-origin products or technology with US-origin components (e.g., modems containing US parts), outside the United States, Oi Personnel must work with the Compliance Team to determine the proper export classification of the item or technology to be exported. The Compliance Team must also determine whether necessary approvals are in place, or authorizations (licenses) are required, to export the item or technology.

3.4 INTERNAL PREVENTION AND CONTROL MEASURES

3.4.1 Financial transactions

All payments made or received must, without exception, be made via electronic transfers to or from bank accounts or bank slips, maintained in the name of the individuals and entities benefiting from the respective payments.

Making or receiving any payment in cash (or equivalent) is prohibited.

As discussed in further detail below, transactions are periodically screened such that transactions involving Sanctioned Persons or Sanctioned Countries, in violation of Sanctions are prohibited.

All transactions or operations suspected of Money Laundering must be immediately forwarded to the Compliance Team for attention and evaluation.

3.4.2 Hiring of Oi Personnel and Contracting with Third Parties Under the Integrity Analysis

The hiring of Oi Personnel and contracting with Third Parties must be carried out following the guidelines of the Integrity Analysis process, which determines that: research must be carried out prior to hiring or contracting, in order to identify any participation or link with persons involved in acts of illicit activities, Money Laundering, Terrorist Financing, located, organized or resident in a Sanctioned Country or on a Restricted Party List. In additional to undertaking an Integrity Analysis upon hiring Oi Personnel or contracting with Third Parties, the Company undertakes a separate comprehensive analysis of existing personnel and parties every twelve months.

The Compliance Team shall make updates to the Integrity Analysis process and identify possible changes to the comprehensive risk assessment annually.

3.4.3 Screenings of Oi Personnel, Third Parties, Counterparties and Transactions Pursuant to Sanctions Policy Procedures

The Compliance Team shall carry out monthly screenings of transactions (including any payments, expenses, income or revenue) to ensure that such transactions do not arise from, any Sanctioned Person or parties otherwise located, organized or resident in a Sanctioned Country; provided that the Compliance Team shall ensure that certain ongoing activities involving embassies of Sanctioned Countries comply with Sanctions and the Company's contractual obligations relating to Sanctions.

In addition, every six months, the Compliance Team shall carry out screenings (in addition to the screenings under the Integrity Analysis) of existing Oi Personnel and Third Parties to ensure their ongoing compliance with Sanctions and Export Control Laws.

The Compliance Team will also screen new Counterparties, and existing Counterparties on a periodic basis and as warranted by updates to the Restricted Party Lists or customer information.

In cases where it is identified that a person has been included on a Restricted Party List or is otherwise in violation of Sanctions or Export Control Laws, their contract will immediately suspended or dealt with in-line with the applicable financing agreement provisions in place.

3.4.4 Additional Third Party Policy Considerations

More detailed anti-corruption and anti-Money Laundering and Terrorist Financing procedures may be carried out whenever necessary to monitor a specific Third Party.

Contracts signed with Third Parties must consider the:

- Clause in which the Third Party certifies that it is aware of the content of this Policy.
- Clause indicating that the Counterparty must declare that it, and none of its Senior Management (or any person(s) whom own(s), control(s), or acts on behalf of the party or its affiliated company) are the subject or target of any Sanctions and Export Control Laws and that the Counterparties (or affiliated companies) have their own procedures in place to combat Sanctions and Export Control violations.

- Clause that provides for the termination of the relationship if non-compliance with the guidelines set out in this Policy is confirmed by the Company and/or in court.
- Clause that provides for the possibility of carrying out in-depth due diligence and additional monitoring, when evidence of possible violation of the guidelines of this Policy, Sanctions or laws are identified.

3.4.5 Training

The Company makes this Policy and its Code of Ethics and Conduct available to all Oi Personnel and Third Parties on the investor relations portal.

Through its education and communication program, the Company offers a training to guide and disseminate a culture of prevention and combating corruption, Sanctions and Export Control Law violations, Money Laundering and Terrorist Financing. The format will vary according to the target audience, and can be online, e-learning or in-person. The training provides an overview of relevant laws pertaining to the Compliance Laws and communicates the compliance responsibilities for relevant personnel.

The education and communication program must be successfully completed by Oi Personnel as soon as reasonably practical after the date hereof, and new Oi Personnel within three months of onboarding. The Company shall obligate Oi Personnel to successfully complete the training and will offer training to Third Parties as deemed necessary. Oi updates the training bi-annually.

3.5 PENALTIES

Oi will consider non-compliance with this Policy as a serious infraction. Oi may impose penalties on Oi Personnel who violate any Compliance Laws, and other applicable laws, or this Policy, including suspension or termination of employment.

3.6 QUESTIONS AND DUTY TO REPORT

Oi supports and encourages people to promptly report any practices that may represent a violation or potential violation of Compliance Laws and other applicable laws, and this Policy. It is worth highlighting that it is everyone's responsibility to uphold Oi's ethical standards and assist in the prevention and detection of all forms of misconduct. If you have any questions or concerns not covered by this Policy, seek guidance from your leader or contact the Compliance Team by e-mail: PP-COMPLIANCE@oi.net.br.

Oi does not tolerate retaliation against any person, internal or external, who reports in good faith a violation or suspected violation of this Policy, applicable laws, the Compliance Laws, or the Company's Code of Conduct.

Oi provides a reporting channel for Oi Personnel and Third Parties who fail, or suspect a failure to comply with Oi's rules and policies, as well as current laws.
Site – http://www.canalconfidencial.com.br/oi/
Phone number – 0800 2822088

If any Oi Personnel believes there has been a violation of any Compliance Laws or other applicable laws, suspects that there may have been a mistake, or is presented with a situation they do not know how to handle, such Company personnel should stop the activity immediately, retain all records, report the situation to the Integrity Committee at 0800 2822088 or http://www.canalconfidencial.com.br/oi/, and await further instruction.

4 ROLES AND RESPONSIBILITIES

Integrity Committee Executives:

- Oversee the Compliance Team and monitor its programs.
- Be aware of and decide on measures regarding suspected violations of the Compliance Laws and Policy.

Compliance Team:

- Carry out Integrity Analysis of Oi Personnel and Third Parties.
- Carry out controls to identify and monitor the Company's relationship with Third Parties, such as to ensure that they are not on Restricted Party Lists or engaged in potential Sanctions or Export Control violations.
- Analyze and report to the Integrity Committee and Audit, Risks and Controls Committee any suspected cases of Money Laundering and/or Terrorist Financing, as well as any identification of relationships with Sanctioned Countries, Sanctioned Persons or violations of Sanctions or Export Control Laws.
- Carry out training and communications programs to raise awareness of Compliance Laws and relevant Company risks and policies.
- Maintain an updated a Compliance clause in the Company's standard contract drafts.

- Ensure that all Oi Personnel and Third Parties are regularly updated on changes to the Compliance Laws.

Audit, Risks and Controls Committee

- Monitor the Policy for effectiveness and non-compliance.
- Upon any confirmation of non-compliance with the Policy, the Committee will take immediate and effective action to ensure that will be developed a solution.

Contracting Areas:

- Submit or request the submission of Third Parties to the Compliance Team's Integrity Analysis.

Oi Personnel:

- Read and follow the guidelines defined in this Policy.
- Successfully compete the Compliance Team training within three months of hiring.
- Report any cases and suspected violations of this Policy or the Compliance Laws to the Compliance Team.

5 RECORDKEEPING

Under US Sanctions laws, records related to transactions involving sanctions-related persons or territories must be kept for a minimum of five years. However, consistent with the statute of limitations, the Company will maintain all due diligence, screening, and other compliance-related records for a minimum of ten years.

6 REFERENCES

- Federal law n° 12.846 of 2013 (Brazilian anticorruption law)
- Federal law nº 9.613 de 1998 (Brazilian money laundering law)
- Federal law nº 13.260 de 2016 (Brazilian anti-terrorism law)
- Oi Code of Ethics and Conduct
- POL-00143 Anticorruption Policy
- POL-00187 Oi Integrity Analysis Policy
- Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. ("FCPA")
- OFAC Sanctions Programs and Country Information
- UK Sanctions and Anti-Money Laundering Act of 2018

7 GLOSSARY

- **Anti-Money Laundering Laws**: means all applicable laws, rules, or regulations relating to terrorism, financial crime or money laundering, including without limitation: (a) the United States Bank Secrecy

Act, as amended by the USA PATRIOT Act of 2001, (b) the United States Money Laundering Control Act of 1986 (18 U.S.C. §§ 1956 and 1957), (c) the Anti-Money Laundering Act of 2020, (d) the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended including pursuant to the Money Laundering and Terrorist Financing (Amendment) Regulations 2019, and € Proceeds of Crime Act 2002, as amended and the rules and regulations (including those issued by any governmental or regulatory authority) thereunder.

- **Contracting Areas**: Any area of the Company and subsidiaries that carries out contracts in accordance with the Purchasing and Contracting Policy.
- **Counterparty:** Parties on the other side of a deal or trade.
- **Export Controls**: means all US and non-US restrictions on the export, reexport, and transfer of certain items, technology, services, and information for national security and foreign policy purposes, including those imposed, administered or enforced from time to time by the US Department of Commerce Bureau of Industry and Security and the US Department of State.
- **Integrity Analysis**: An extensive preventive analysis process of reputation and integrity risks in relationships with employees, suppliers, service providers, partners, sponsors and beneficiaries of the Company, based on risk criteria, integrity maturity analysis, negative media and presence on Restricted Party Lists. The analysis contains a broader assessment of anti-corruption and bribery and Sanctions risks that goes beyond screening measures. The scope of the Integrity Analysis is described in the Integrity Analysis Policy.
- **Oi Personnel**: For the purposes of this Policy, it includes all Company employees, (including managers, officers, directors, board members).
- **OFAC**: The US Department of Treasury's Office of Foreign Assets Control.
- **Restricted Party Lists**: These are international lists that identify organizations and individuals involved in illicit activities such as Money Laundering, Terrorist Financing, economic crimes, Sanctions violations and other legal irregularities. The US, EU and EU member states and UK and United Nations Security Council lists selected by the Compliance team to be taken into consideration in third-party integrity analysis, include the:
  - US Office of Foreign Assets Control
    - Specially Designated Nationals and Blocked Persons List (SDN List)
    - Foreign Sanctions Evaders List (FSE List)
    - Sectoral Sanctions Identifications List (SSI List)
  - US Bureau of Industry and Security
    - Denied Persons List

    - Entity List
    - Unverified List
  - US Department of State
    - Department of State List of Sanctioned Entities (Non-Proliferation)
    - Department of State Debarred Parties List.
  - UK Office of Financial Sanctions Limitations
    - Consolidated Lists
  - European Commission
    - Consolidated Lists
- **Sanctions**: Means any financial or economic sanctions, embargoes or similar restrictive measures, administered or enforced by the United States (including the US Department of the Treasury's Office of Foreign Assets Control, the US Department of Commerce and the US Department of State), the United Nations Security Council, the European Union and any European Union member state, or His Majesty's Treasury of the United Kingdom.
- **Sanctions and Export Control Laws**: Means any financial or economic sanctions, embargoes or export controls or similar restrictive measures, administered or enforced by the United States (including the US Department of the Treasury's Office of Foreign Assets Control, the US Department of Commerce and the US Department of State), the United Nations Security Council, the European Union and any European Union member state, or His Majesty's Treasury of the United Kingdom.
- **Sanctioned Country**: a country or territory that is the subject or target of comprehensive Sanctions (currently, the so-called Donetsk People's Republic, or the so- called Luhansk People's Republic, and the Crimea, Kherson and Zaporizhzhia regions of Ukraine, Cuba, Iran, North Korea and Syria).
- **Sanctioned Person**: means any Person that is, or is owned or controlled by, or acting on behalf of, one or more persons that are: (i) the subject or target of any Sanctions, or (ii) located, organized or resident in a country or territory that is the subject or target of comprehensive Sanctions (currently, the so-called Donetsk People's Republic, or the so- called Luhansk People's Republic, and the Crimea, Kherson and Zaporizhzhia regions of Ukraine, Cuba, Iran, North Korea and Syria).
- **Senior Management**: Executives who report directly to the president and members of the Company's Boards.
- **Terrorist Financing**: It happens when terrorist organizations and/or countries that host these organizations benefit from the allocation of resources that can be used in the planning, preparation or practice of Terrorism. Resources can be of legal origin (through the hiring of Third Parties or services, personal donations and company profits) or of illicit origin (through criminal actions).

- **Third Party**: Any and all service providers, agents, suppliers, consultants, or business partners, whether individuals or legal entities, who act on behalf of the Company, by proxy or not.

8 ATTACHMENTS

Not applicable.

9 APPROVAL

Approved by	Approval date
Board of Directors	07/31/2024

THIS DOCUMENT REPEALS PREVIOUS VERSIONS