1. DEFINITIONS

For the purposes of this Policy, the following terms shall have the meanings assigned to them below:

Term	Acronym	Definition
BRN	BRN	Brazilian Nickel Limited
BRN Group		BRN and its subsidiaries
Ultimate Beneficial Owner	BF	An individual who ultimately owns, controls, or benefits from the activities of a legal entity or an entity without legal personality.
Money Laundering	ML	The practice of illegal activities aimed at transforming funds obtained through illegal activities into funds with an apparently legal origin, by concealing or disguising the nature, origin, location, disposition, movement, or ownership of property, rights, or values derived, directly or indirectly, from criminal offenses.
Terrorism Financing	FT	Financial support, by any means, for terrorism or those who encourage, plan, or commit acts of terrorism.
Anti-Money Laundering / Countering-Terrorist Financing	AML / CTF	Set of laws, regulations, and procedures to prevent money laundering and terrorist financing.
Proceeds of Crime Act	POCA	UK legislation dealing with the recovery of assets obtained through criminal activities.
Terrorism Act	Act 2000	British law that gives authorities powers to trace, freeze, and confiscate criminally obtained assets, strengthening the fight against money laundering and organized crime.
Sanctions and Anti-Money Laundering Act 2018	SAMLA 2018	UK law regulating the imposition of sanctions and combating money laundering, especially after Brexit (the UK's exit from the European Union).
Brazilian Law No. 9,613/1998	-	Anti-Money Laundering Law, which provides for crimes of "laundering" or concealment of assets, rights, and values; the prevention of the use of the financial system for the illegal activities provided for in this Law; creates the Council for Financial Activities Control (COAF), and makes other provisions.
Law 13,260/2016	-	Regulates the provisions of item XLIII of Article 5 of the Federal Constitution, disciplining terrorism, dealing with investigative and procedural provisions, and reformulating the concept of terrorist organization; and amends Laws No. 7,960, of December 21, 1989, and

		No. 12,850, of August 2, 2013.
Money Laundering Regulations	MLR 2017	Set of rules implemented in the United Kingdom to prevent money laundering and terrorist financing, in force in conjunction with the Proceeds of Crime Act 2002 (POCA) and the Terrorism Act 2000.
Counterparty Due Diligence	CDD	Due diligence is a process of detailed investigation and analysis of documents and information aimed at evaluating a business partner, supplier, or customer, which will serve as support for decision-making.
Risk Assessment	-	Analysis of a company's potential exposure to financial crime based on customers, products, and location.
Suspicious Activity		Any operation, conduct, transaction, or set of transactions that, due to its nature, value, frequency, complexity, or lack of economic or legal justification, may indicate evidence of money laundering, concealment of assets, rights, and values, fraud, corruption, or terrorist financing. Examples of suspicious activities include: • Transactions incompatible with the financial capacity or usual profile of the counterparty; • Use of complex or unusual corporate structures without plausible justification; • Payments in cash or by means that make traceability difficult; • Sudden changes in final beneficiaries without valid justification; • Unjustified refusal to provide information or documents required for due diligence; • Relationships with individuals or legal entities included in restrictive lists, sanctions lists, or politically exposed persons (PEPs) lists, without adequate risk mitigation.
Representatives	-	Persons who officially act on behalf of BRN and/or its Subsidiaries (through instruments that formally grant such powers), such as employees, directors or managers, hired consultants, service providers, or partners.
Politically Exposed Person	PPE	This refers to an individual who holds or has held a relevant national or international public office, who is therefore at a higher risk of involvement in corruption, bribery, or money laundering.
Entity	-	Any organization or formal structure that has legal or recognized existence and can act on its own behalf. It can be either for-profit or non-profit, and may or may not have legal personality.
Subsidiary		A company controlled by BRN, which has decision-making power over its operations and strategies.
Tax Havens		Countries or territories that offer very low or no taxation, strong banking and corporate secrecy, and flexible financial regulation, attracting individuals and legal entities who wish to reduce taxes or, allegedly, hide assets.

2. OBJECTIVES

This Policy has the following objectives:

a) to establish guidelines for preventing and combating money laundering and terrorist financing crimes, in accordance with applicable national and international laws and regulations;
b) ensure compliance with national and international laws and regulations related to the prevention and combating of money laundering and terrorist financing;
c) promote a culture of integrity, ethics, transparency, and compliance, reinforcing the institutional commitment to preventing financial crimes and combating terrorism;

3. APPLICATION

This Policy applies to all individuals working in BRN Group companies and their subsidiaries, at all hierarchical levels, including managers, senior staff, executives, directors, employees (permanent or temporary), apprentices, and interns.

The guidelines of this Policy must also be observed by partners, suppliers, and outsourced service providers, or any other individual or legal entity that has a relationship with any BRN Group company.

4. KEY DEFINITIONS

4.1 MONEY LAUNDERING (ML)

Money laundering consists of illegal activities that aim to transform funds obtained through illegal activities into funds with an apparently legal origin, by concealing or disguising the nature, origin, location, disposition, movement, or ownership of goods, rights, or values derived, directly or indirectly, from criminal offenses.

The money laundering process can involve three stages:

a) **Placement:** This consists of introducing illicit funds into the economic system. To this end, a wide variety of operations are carried out, such as deposits into bank accounts, possibly in small amounts and held by third parties; conversion into foreign currency; purchase of financial products and services; investments in savings and/or investment funds; purchase of assets such as real estate, gold, precious stones, works of art, among others.

b) **Concealment:** This consists of carrying out multiple financial transactions aimed at concealing illegal funds, with the objective of distancing the amounts from their illicit origin. This phase can take place through complex and numerous transactions to make it difficult to trace, monitor, and identify the illegal source of the money. In this phase, it is common to make bank transfers between accounts located in different countries, with the destination often being countries considered tax havens.

c) **Integration**: This consists of formally incorporating the funds into the economic system through investment in the capital, financial, real estate, and art markets, among others. At this stage, assets of illicit origin are already mixed or incorporated with legitimately obtained funds and are used in lawful or unlawful businesses, either in legitimate transactions or in simulated transactions, such as false import/export operations, the purchase and sale of real estate at prices different from market values, reverse loans, etc.

4.2 TERRORIST FINANCING (TF)

Terrorist financing is the financial support, by any means, of terrorism or those who encourage, plan, or commit acts of terrorism.

This fundraising can take many forms, particularly illicit sources such as drug trafficking, arms smuggling, prostitution, organized crime, fraud, among others.

Examples of FT violations: soliciting funds, receiving or providing money or other property, knowing or having reasonable grounds to suspect that it will or may be used for terrorist purposes; entering into or engaging in arrangements whereby money or other property is made available to another person, with reasonable grounds to suspect that it will or may be used for terrorist purposes; entering into or engaging in an arrangement that facilitates the retention or control of terrorist property by concealing it, removing it from the jurisdiction, transferring it to nominees, or doing anything else to achieve this.

The fight against terrorist financing is closely linked to the fight against money laundering, as the techniques used to launder money are essentially the same as those used to conceal the origin and destination of terrorist financing.

5. GUIDELINES

The following guidelines are established at BRN and its Subsidiaries:

a) Develop and disseminate, on an ongoing basis, to its employees and third parties, knowledge and a culture of preventing and combating terrorist financing, money laundering, and the concealment of assets, rights, and values;

b) Define *Due Diligence* and Continuous Monitoring procedures for detecting of atypical and/or suspicious transactions that may constitute evidence of terrorist financing or money laundering or concealment of assets, rights, and values;

c) Establish internal reporting processes for suspicious activities, using the Internal Suspicious Activity Report Form (see Annex B);

d) Ensure the application of disciplinary sanctions and corrective measures in case of non-compliance with the guidelines established in this Policy, as well as in the legislation applicable to BRN and/or its subsidiaries;

e) Promote periodic training and capacity building on this Policy, in accordance with national and international legislation applicable to BNR and/or its Subsidiaries, in order to keep knowledge up to date and disseminate good prevention practices;

f) Maintain adequate records and documentation, ensuring traceability and compliance with legal retention periods.

6. APPLICABLE LEGISLATION

This Policy complies with national and international standards, such as, but not limited to:

a) **Proceeds of Crime Act 2002 (POCA), Part 7:** UK legislation on the main money laundering offenses, as well as offenses that apply to regulated sectors. Under this legislation, and for the purposes of this Policy, it is also an offense to attempt, conspire, incite, aid, encourage, advise, or procure the commission of a principal money laundering offense.

b) **Part 2 of the Terrorism Act 2000**: provides for similar offenses related to terrorist financing, in particular offenses of fundraising, use and possession, financing arrangements, money laundering, and terrorist financing. The UK's Counter Terrorist Financing regime runs in parallel with the UK's Anti-Money Laundering regime.

c) **The Sanctions and Anti-Money Laundering Act 2018 (SAMLA)** is the legislation that allows the UK to impose sanctions and implement standards related to combating threats to the integrity of the international financial system. Several regulations have been

introduced under SAMLA, such as the 2021 Global Anti-Corruption Sanctions Regulations, the Anti-Terrorism Regulations, the Russia Sanctions Regulations, and additional regulations issued through 2025 covering digital assets, luxury goods, and high-risk transactions in emerging sectors.

d) **Brazilian Law No. 9,613/1998**: establishes measures aimed at preventing and suppressing money laundering crimes, defined as the practice of concealing or disguising the origin of assets, rights, or values derived from illicit activities. Its main objective is to prevent the national economic and financial system from being used to legitimize criminally obtained funds, through mechanisms such as customer identification, monitoring of operations, and reporting of suspicious transactions to the competent authorities.

e) **Brazilian Law No. 13,260/2016**: regulates the provisions of item XLIII of Article 5 of the Federal Constitution, which deals with crimes that are not eligible for bail and are not subject to pardon or amnesty, such as the practice of torture, illicit trafficking in narcotics and related drugs, terrorism, and crimes defined as heinous, for which the instigators, perpetrators, and those who could have prevented them but failed to do so are liable, regulating terrorism, dealing with investigative and procedural provisions, and reformulating the concept of a terrorist organization; and amends Laws No. 7,960, of December 21, 1989, and No. 12,850, of August 2, 2013.

f) **Law 13,810/2019** provides for compliance with sanctions imposed by United Nations Security Council resolutions, including the freezing of assets of individuals, legal entities, and organizations, and the national designation of persons investigated or accused of terrorism, its financing, or related acts.

7. DUTIES AND RESPONSIBILITIES

The duties and responsibilities under this Policy are as follows:

1. **BRN Board of Directors**
    - Ensure the availability of adequate resources for the implementation of measures to prevent money laundering and terrorist financing.
    - Promote a culture of compliance and ethics throughout the organization (BRN and Subsidiaries).

- Act cooperatively with national and international authorities to combat money laundering and terrorist financing, facilitating, at all times, in accordance with the applicable legal provisions in force in each jurisdiction, the documentation and information required by such authorities.

2. **Compliance Responsible, and, in the absence thereof, the Legal and Governance Officer.**
   - Periodically review this policy;
   - Implement, supervise, and update the internal controls provided for in this Policy, namely the procedures for Internal Reporting of Suspicious Activity, Counterparty Due Diligence, and Red Flag alerts.
   - Monitor suspicious transactions, receive Internal Suspicious Activity Report Forms, ensuring they are sent to the Procurement Committee for deliberation and communication to the competent authorities, when applicable.
   - Forward cases in which the DDC assesses the supplier as "high risk" under the terms of item 8.2 of this policy to the Procurement Committee for deliberation;
   - Ensure periodic and adequate training for employees.
   - Act as a point of contact with regulatory and supervisory authorities.

3. **Supply Department**
   - Perform supplier *due diligence* processes and, when applicable, forward reports on suppliers classified as High Risk for evaluation by the financial, compliance, or legal teams, in accordance with item 8.2 of this policy.
   - Include supplier approvals/disapprovals in the software used to record Counterparty *Due Diligence*, validating the decisions made by the compliance, legal, financial teams or by the Procurement Committee.

4. **Managers and Immediate Supervisors**
   - Ensure compliance with this Policy in their respective areas.
   - Guide their teams on procedures for preventing money laundering and terrorist financing.
   - Report any suspicious activity using the Internal Suspicious Activity Report Form to the manager or directly to the Compliance Responsible, and, in the absence thereof, the Legal and Governance Officer.

5. Employees in General

- Comply fully with the guidelines and procedures set forth in this Policy.
- Participate in mandatory training.
- Report any suspicious activity using the Internal Suspicious Activity Report Form to the manager or directly to the Compliance Officer and, in their absence, to the Legal and Governance Director.

6. Third Parties (suppliers, service providers, in any capacity)

- Observe this Policy and applicable laws during the performance of their activities.
- Cooperate with BRN and its Subsidiaries in the prevention and detection of money laundering and terrorist financing risks.
- Provide any necessary clarifications and information during the *due diligence* process.

8. PROCEDURES

BRN and its subsidiaries will adopt effective measures to prevent and combat money laundering and terrorist financing crimes.

Ultimate Beneficiaries are persons who own or control a counterparty and/or the person on whose behalf a transaction is carried out. The determination of the Ultimate Beneficiary aims to discover the individuals who control or benefit from the legal entity or center of collective interests without legal personality.

To establish the Ultimate Beneficial Owner, BRN and its Subsidiaries will establish procedures for Internal Reporting of Suspicious Activity, Counterparty *Due Diligence,* as well as alerts for *Red Flags*, as specified below.

8.1 INTERNAL REPORTING OF SUSPICIOUS ACTIVITIES (“RAS”)

BRN and its subsidiaries will maintain a formalized process for the internal reporting of suspicious activities, using the Internal Suspicious Activity Report Form (RAS - see Annex B).

The form may be completed with the identification of the complainant or anonymously, with the information being treated with absolute confidentiality and any form of retaliation prohibited, in which case it will be forwarded through the complaints channel.

The forms shall be forwarded by the Compliance Responsible, and, in the absence thereof, the Legal and Governance Officer to the Secretariat of the Procurement Committee, which is responsible for recording the occurrence, consolidating the information, and including the case on the Committee's meeting agenda.

The Procurement Committee shall review and deliberate on the complaints and RAS forms received within a maximum period of thirty (30) days from the date of receipt of the RAS form.

The Committee may deliberate on the following measures: (i) closing the case, (ii) initiating an internal investigation, (iii) referring the case to the Legal Department when there is a need for legal assessment, support in internal investigations, or interaction with authorities, or (iv) communicating with the competent authorities, when applicable.

All records and deliberations related to RAS forms shall be filed by the Committee Secretariat in a secure repository for audit and traceability purposes.

8.2 COUNTERPARTY DUE DILIGENCE (CDD)

Counterparty *Due Diligence* aims to identify the true beneficiaries or individuals who exercise control over illicitly obtained assets or who finance criminal activities, in order to curb money laundering and terrorist financing activities, and will be performed on all suppliers (including any third parties interested in doing business with BRN and/or its Subsidiaries) using supplier risk management software.

The DDC includes procedures for assessing risk in contracting, including reputational and financial assessment, which will evaluate the points described in Annex A - Counterparty Assessment Criteria.

At the end of the DDC, the supplier will be classified as Low, Medium, or High risk. If the classification is **High risk**, the registration of this supplier must be automatically rejected or, in cases where an assessment is necessary, the DDC report must:

a) be forwarded to the Compliance team or, in its absence, to the legal team (reputational assessment) or financial team (financial assessment) for preliminary assessment of the supplier in order to confirm the risk classification indicated by the Software;
b) if the High risk classification is maintained, the DDC will be forwarded to the Procurement Committee for approval or rejection of the supplier's registration.

The Procurement Committee shall:

- Evaluate the information provided or made available in the DDC;
- Take additional measures to better understand the background, ownership, and financial situation of the counterparty and other parties to the transaction;
- Take additional measures to certify that the transaction, if carried out, will be consistent with the intended purpose and nature of the business relationship, in a lawful and legitimate manner, or
- Request monitoring of the business relationship, including increased scrutiny of transactions.
- Other measures deemed necessary.

8.3 RED FLAGS

In order to guide and facilitate the identification of suspicious activities or transactions, the following is a list of activities considered to be "red flags," without prejudice to others, depending on the specific case, which should be reported to the Procurement Committee using the Internal Suspicious Activity Report Form (see Appendix A).

1. **Customer or Counterparty**

- Reluctance to provide identification information or required documentation (KYC).
- Use of apparently false or inconsistent documents.
- Absence of a business address.
- Complex corporate structures with no apparent economic justification.
- Clients who insist on not formally registering the contractual relationship.

2. **Financial Transactions**

- Transactions incompatible with the customer's financial capacity or declared profile.
- High-value transactions carried out in cash or virtual assets, without reasonable justification.
- Fragmented payments or receipts ("smurfing") to avoid reporting limits.
- Frequent transfers to or from jurisdictions considered high risk (e.g., countries or territories where anti-money laundering and counter-terrorist financing controls are weak, financial supervision is limited, which may mean high levels of corruption or political instability, and transparency standards are not those required by the BRN Group). Or non-cooperative.
- Involvement of accounts or intermediaries with no apparent connection to the transaction to be carried out.

3. **Behavior and Conduct**

- Customer or partner demonstrates unusual haste to complete a transaction.

- Refusal to clarify the economic or commercial purpose of the transaction.
- Negative or aggressive reactions when questioned about the origin of the funds to be used in the transaction.
- Attempts to offer undue advantages to facilitate the transaction (which may include, but is not limited to, direct payment to the employee or anyone they designate, gifts, presents, or hospitality, etc.).
- Is related to a person listed as involved or suspected of involvement in terrorist activities or activities related to terrorist financing.
- Appears to be instructed by a third party whose identity is not disclosed.
- Involvement of BRN and its subsidiaries from another jurisdiction, without justification for doing so.
- Uses an email address with an unusual domain or one that is more appropriate in the context of the transaction, such as Hotmail, Gmail, Yahoo, etc.
- Expresses conduct of not obtaining the necessary government approvals/filings.

4. **Third Parties and Business Partners**

- Partners with no verifiable history or reputation.
- Front companies or newly created companies with no real operational activity.
- Frequent changes in partners, address, or organizational structure without justification.
- Business relationships involving unnecessary intermediaries or excessive commissions.

5. **Risk Sectors and Products**

- Transactions involving sectors highly susceptible to money laundering (e.g., gaming, luxury real estate, precious metals, works of art).
- Products or services that allow anonymity or the use of untraceable cryptocurrencies.

The above list is not exhaustive or comprehensive, but provides some factors that raise concerns about suspicious activities and does not exempt recipients of this policy from paying attention to any other warning signs that require further investigation.

8.4 CONTINUOUS MONITORING

BRN and its subsidiaries will continuously monitor their business relationships by permanently performing Counterparty Due Diligence (CDD) processes, analyzing *Red Flags*, and using the Internal Suspicious Activity Report Form.

This monitoring aims to identify, assess, and mitigate money laundering and terrorist financing risks in a timely and systematic manner.

Cases classified as suspicious will be forwarded by the Compliance Responsible, and, in the absence thereof, the Legal and Governance Officer to the Procurement Committee, which is responsible for analyzing them and deciding on the appropriate measures.

Monitoring may also include the integration of artificial intelligence technologies and automated anomaly detection systems to analyze unusual transaction patterns.

9. TRAINING

BRN and its Subsidiaries' employees must receive adequate and mandatory training on this policy as part of their onboarding process, as well as on how to implement and adhere to this Policy.

It is reiterated that BRN and its subsidiaries have zero tolerance for conduct practiced for the purposes of money laundering and terrorist financing and are committed to taking all appropriate measures to stop any conduct that results in non-compliance with this Policy.

10. FILING

BRN and its Subsidiaries will maintain records of all *Counterparty Due Diligence* documents, Internal Suspicious Activity Report Forms, and deliberations of the Procurement Committee, as well as all supporting information and records related to any transaction that is subject to ongoing monitoring.

11. APPENDICES

Counterparty Due Diligence Evaluation Criteria - *CDD* (Appendix A).

Internal Suspicious Activity Report Form (Appendix B)

12. CONTROL AND REVIEWS

The BRN Board of Directors will periodically monitor the implementation and functioning of this policy, considering its adequacy and effectiveness.

All employees are responsible for the success of this policy and must ensure that they use it to report any suspected risks or irregularities.

Employees and third parties are invited to comment on this policy and suggest ways in which it can be improved. Comments, suggestions, and questions should be addressed to *the Legal and Governance Officer.*

The updated version of the policy will be immediately available on the BRN intranet and communicated via corporate email.

Review	Date	Reason for revision	Prepared by	Reviewed by
Rev. 01	11/30/2022	Initial issue	Adrian Harvey	Mike Oxley
Rev. 02	20/10/2025	Update	Sílvia Araujo (Senior Lawyer)	Robert Willetts (Chief Legal & Governance Officer)

SCHEDULE A

COUNTERPARTY EVALUATION CRITERIA

	Reputational Analysis	Financial Analysis
Registration Data and Structure	Field of activity; Location (headquarters and branches); Subsidiaries and affiliates; Family Tree; Ultimate beneficiary; Number of employees; Corporate structure; Website; Telephone numbers; Email; Length of operation	Field of activity; Company history; Location (headquarters and branches); Subsidiaries and affiliates; Number of employees; Information on partners/directors; Corporate structure; Website; Telephone numbers; Email; Operating hours
Legal proceedings	Criminal actions; Civil actions	Search and seizure actions; Tax actions
Commercial Proceedings		National commercial references; Consultations in the last 12 months (domestic and international); Protests; Returned checks; Judicial reorganization; Bankruptcy (requested/declared); Commercial disputes and refinancing
Due Diligence	CEIS (Register of Reputable and Suspended Companies); CEPIM (Register of Non-Profit Private Entities); CNEP (National Register of Punished Companies) Transparency Portal (leniency agreements); CEAF (Federal Administration Expulsion Registry); General List of Disqualified Entities (Central Bank); PROCON (Consumer Protection and Defense Program); MPF Proceedings (Legal Proceedings); Irregular Accounts System (TCU) International Lists (UN, OFAC, DFAT, etc.); PEP (Politically Exposed Person) Adverse media	
Certificates	Federal, State, Municipal, FGTS, Labor Debts, CNIA-CNJ, Negative Report on Unsuitable Bidders (TCU), IBAMA (debts, compliance, embargoes/fines), Denial of Proceedings (TCU)	Federal Taxes, State, Municipal, FGTS, Labor Debts
Economic/Financial	Actual annual revenue; Net profit; Total assets	Estimated annual revenue; Actual annual revenue; Credit limit
Scope of verification (includes partners and directors)	Up to 13 names including: -company name, -trade name, -former company name, -up to 5 partners/shareholders, -up to 5 directors/executives	
Classification	Low Risk Medium Risk High Risk	Score 0-100 Low Risk Medium Risk High Risk

SCHEDULE B

INTERNAL SUSPICIOUS ACTIVITY REPORTING FORM (SAR)

Confidential

1. Reporter's details (optional, if anonymity is desired)

- Name: _____
- Area/department: _____
- Position/Function: _____

---

2. Suspicious Incident Details

- Date of Identification: //_____
- Location: _____
- Individuals Involved (if any): _____

---

3. Description of Suspicious Activity

( ) Unusual financial transaction
( ) Payment without adequate justification
( ) Supplier/customer with no clear history or high risk
( ) Evidence of fraud or contractual irregularity
( ) Relationship with politically exposed person (PEP)
( ) Other: _____

Detailed description of the fact:

---

4. Attached Documents/Evidence

( ) Contracts/internal documents
( ) Proof of payment/transaction
( ) Emails/communications
( ) Other: _____

---

5. Preliminary Analysis (to be completed by the Compliance Officer or, in their absence, by the Director of Governance and Procurement)

- Record No. _____
- Date of Protocol: //_____
- Compliance with formal requirements: ( ) Yes ( ) No
- Forwarded to the Committee on: //_____

---

6. Deliberation of the Governance and Compliance Committee

- Decision:
  ( ) File away (insufficient evidence)
  ( ) Order additional internal investigation
  ( ) Notify Legal
  ( ) Notify the Competent Authorities
  ( ) Other: _____
- Responsible for implementing the decision: _____
- Deadline: //_____

---

7. Registration and Filing

- Signature of the Committee Secretariat: _____
- Date of case closure: //_____