1. Objective

This PRIVACY AND PERSONAL DATA PROTECTION POLICY ("POLICY") aims to establish general guidelines to ensure the privacy and protection of personal data to which MINERAÇÃO TABOCA S.A. ("TABOCA" or "COMPANY") has access, as well as to reaffirm the commitment to information security for all actors involved in its activities, whether they are customers, business partners, service providers, or third parties, in accordance with the Brazilian General Data Protection Law ("LGPD").

This Policy aims to describe the procedures and/or conduct that ensures and reinforces TABOCA's commitment not only to the LGPD but also to the practices and regulations to be followed during the conduct of activities and operations for the Processing of Personal Data carried out by the COMPANY and the recipients of this Policy.

2. Scope

This Policy applies to all employees, collaborators, third parties, interns, directors, service providers, suppliers, and any other persons who have access to personal data through TABOCA ("Members").

3. Terms and Definitions

Below are the main terms adopted in this Policy, along with their respective meanings:

1. Personal Data: Any information related to an individual that identifies or may identify them, including, for example, name, surname, nickname, age, residential or electronic address, location data, vehicle license plates, purchase profiles, academic data, purchase history, among others.
2. Sensitive Personal Data: Data related to the characteristics of an individual's personality and/or personal choices that may result in discrimination, such as racial or ethnic origin, religious belief, political opinion, membership in a union or religious, philosophical, or political organization, health or sex life data, genetic or biometric data when linked to a natural person.
3. Data Subject: The individual to whom Personal Data and/or Sensitive Personal Data refers, which is subject to any Processing.
4. Processing: Any operation or set of operations performed with Personal Data, by automated or non-automated means, such as collection, registration, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, transfer, dissemination or otherwise making available, alignment or combination, blocking, deletion, extraction, elimination, or destruction.
5. Database: A structured set of Personal Data, established in one or more locations, in electronic or physical support.
6. Anonymization: The use of reasonable and available technical means at the time of Processing, by which data loses the possibility of association, directly or indirectly, with an individual.
7. Anonymized Data: Data related to a Data Subject that cannot be identified, considering the use of reasonable and available technical means at the time of its Processing.
8. Legal Basis: Legal justification that legitimizes the Processing of Personal Data for a specific purpose, under Brazilian Law.
9. Brazilian Law: All current legal norms related to the protection of Personal Data, including but not limited to: the Federal Constitution of Brazil; Lei Geral de Proteção de Dados (Lei nº 13.709/2018); Marco Civil da Internet (Lei nº 12.965/2014); Decreto Regulamentador do Marco Civil da Internet (Decreto nº 8.771/2016); Código Civil (Lei nº 10.406/2002), Código de Defesa do Consumidor (Lei n° 8.078/90); Lei de Acesso à Informação (Lei nº 12.527/2011);

10. General Data Protection Law (Lei Geral de Proteção de Dados, "LGPD"): Regulates the Processing of Personal Data, in physical and digital means, by a natural person or a legal entity of public or private law.

11. National Data Protection Authority ("ANPD"): Special federal agency responsible for overseeing compliance with the General Data Protection Law in Brazil.

12. Data Controller: An individual or entity that, alone or in conjunction with others, determines the purposes and means of Processing Personal Data of Members.

13. Data Processor: Refers to an individual or legal entity that processes Personal Data on behalf of the Data Controller.

14. Data Protection Officer (DPO): An individual or entity appointed by TABOCA as a communication link between the Data Controller, the Data Subjects, and the ANPD.

15. Third Parties: All those who do not belong to TABOCA's organizational structure.

16. International Transfer: Transfer of Personal Data to a foreign country or international organization of which the country is a member.

17. Information Security Incident: Any confirmed adverse event related to the breach of personal data security, such as unauthorized, accidental, or unlawful access that results in destruction, loss, alteration, leakage, or any form of inappropriate or unlawful Processing of Personal Data, which may pose a risk to the rights and freedoms of the Data Subject.

4. Principles of Personal Data Processing

In the Processing of Personal Data, TABOCA will consider and respect the following legal principles:

1. Adequacy: The processing of personal data must be compatible with the purpose informed to its Data Subject; that is, it must be aligned with the intended purposes for the scope.
2. Purpose: Personal data must be collected for a specific, explicit, and legitimate purpose at the time of collection. Thus, the Personal Data collected should not be used for any purpose other than that informed to its Data Subject.
3. Legality: The processing of personal data will only be considered legal if based on at least one of the legal bases provided for in applicable legislation.
4. Free Access: The Data Subject must be guaranteed facilitated and free access to information regarding how their personal data is processed and the duration of such processing.
5. Non-Discrimination: Personal data should not be processed for discriminatory, illegal, or abusive purposes.
6. Need: Limitation of personal data processing to the minimum necessary to achieve its purpose, avoiding excessive processing of personal data.
7. Prevention: Measures must be adopted to prevent the occurrence of harm resulting from personal data processing.
8. Quality: The personal data processed must be accurate, clear, relevant, and up to date according to the needs and for the fulfillment of its processing purpose.
9. Accountability: The data controller must ensure compliance and demonstrate conformity of each personal data processing operation with the requirements established in applicable legislation.
10. Security: The processing of personal data must consider the necessary security against unauthorized or improper processing, and against loss, destruction, and accidental damage, using adequate technical and organizational measures.
11. Transparency: The Data Subject must be aware of and be informed in advance of who the Data Controller(s), Processor(s), DPO, and Third Parties who may receive their personal data are, as well as the purpose(s) of the processing.

5. Responsibilities and Authorities

5.1. Personal Data Protection

All employees of TABOCA, whether permanent or temporary, business partners, service providers, and Third Parties acting on its behalf, must comply with all provisions in current legislation and internal procedures regarding the protection of personal data and the protection of the rights and freedoms of the Data Subjects, whose personal data may be processed in their professional activities.

5.2. Personal Data Processing

In the exercise of its activities, provided that the standards and guidelines of this Policy are met, TABOCA may use Personal Data for recruitment/selection of individuals; to register, identify, and monitor access to its establishments; to prepare management reports of its projects; to carry out business partnerships, contracts, development, and compliance of the services provided; as well as to conduct Email Marketing ("Mailing") to contact the Data Subject through newsletters, promotional materials, and other means.

5.3. Sensitive Personal Data Processing

In TABOCA's operations, the Processing of Sensitive Personal Data will be carried out for the following purposes:

1. Completing forms containing personal information (ID, CPF, marital status, birthplace, profession, residential address);

2. Digital and facial biometrics;

3. Medical documents control (e.g., pre-employment medical exams, toxicology tests, COVID-19 tests, and other occupational medical exams);

4. Completing forms with personal information in its Database (e.g., passport number).

TABOCA also recognizes the relevance and specificity involved in the Processing of Sensitive Personal Data and, for this reason, commits to adopting special safeguards

6. Activities

6.1. Legal basis

The Personal Data Processing in TABOCA's operations scope is based on legal grounds, as provided for in the LGPD. Thus, primarily, the legal basis must be identified and recorded. Processing without any legal basis or legal foundation may be considered irregular and must be immediately interrupted. Processing may be supported by at least one of the Legal Bases described below:

1. Prior consent from the Data Subject;

2. Compliance with a legal or regulatory obligation;

3. When necessary for a contract execution or preliminary procedures related to a contract to which the Data Subject is a party, at the request of the Data Subject;

4. Compliance with a task carried out in the public interest or for the regular exercise of rights in judicial, administrative, or arbitral processes;

5. For Data Subject or third parties life protection or physical safety;

6. Legitimate interest, except when fundamental rights and freedoms of the Data Subject prevail, requiring the protection of Personal Data.

6.2. Data Subject Rights

Members may request TABOCA access to information regarding:

1. Personal Data Processing maintained and/or possibly disclosed or transferred; regarding the right to oppose, restrict, stop, or prevent Processing;

2. The right to correct any errors in their Personal Data;

3. The right to delete Personal Data from the Personal Data Databases, except for legal storage obligations;

4. The right to receive their Personal Data in a structured, readable format;

5. The right to revoke their Consent for the Purposes of Processing Personal Data linked to them;

6. The right to information about the developments in their relationship with TABOCA;

7. The right to Personal Data portability, upon request, so that the Personal Data under Processing can be transferred to another service provider indicated by the Data Subject; and

8. The right to anonymization or blocking, upon prior request.

Requests should be addressed to the Data Protection Officer at the email: lgpdmtaboca@mtaboca.com.br.

However, it is important to note that TABOCA is subject to legal obligations imposed by the LGPD and other regulatory norms and obligations, so some requests may not be fulfilled.

6.3. Personal Data Security

A TABOCA commits to making its best efforts to

- Implement and maintain physical, technical, and organizational measures appropriate to protect its Members Personal Data, service providers, partners, and customers from unauthorized access and accidental, internal or external, or unlawful destruction situations, loss, alteration, communication, or any improper or unlawful form Processing of such information;
- Regularly monitor its systems and networks, making all reasonable efforts to identify, mitigate, and neutralize vulnerabilities and attacks;
- Ensure that Personal Data Processing activities are conducted only by Members and/or third parties authorized and properly trained to comply with the obligations established herein and with relevant Policies;
- Adopt necessary security measures to safeguard operations in line with the technologies available in the market at the time of the activity;
- Have an action plan in place for Information Security Incidents, whether physical or digital.

Access to information on TABOCA's networks will be limited based on user profiles created by technical support according to each Member's functions, with prior approval.

If a Member notices any Information Security Incident related to their work routine, on devices provided by TABOCA or their own, they must immediately contact TABOCA's Information Technology team.

The Information Technology (IT) team can be contacted through the following channel: Email: si@mtaboca.com.br.

6.4 Personal Data Disclosure and Transfer to Third Parties

Disclosures will be allowed when the information is requested for one or more of the following situations, which are listed as examples:

1. To comply with TABOCA's legal or regulatory obligation;

2. Shared processing of Personal Data necessary for the execution of public policies provided for in laws or regulations by public administration;

3. Regular exercise of rights, including under contract and in judicial, administrative, and arbitral proceedings, in accordance with applicable laws;

4. Data Subject or third parties life or physical safety protection;

5. When it is necessary to meet the legitimate interests of TABOCA or third parties, except when the fundamental rights and freedoms of the Data Subject prevail, requiring the protection of Personal Data.

Thus, all requests for the provision of Personal Data based on the above situations must be supported by appropriate documentation and specifically authorized by the Data Protection Officer.

6.5 Personal data transfer and processing to foreigners

In the event of Processing Personal Data of Foreigners and/or International Transfer of Personal Data, TABOCA must evidence and formalize the Processing or transfer, as applicable, in accordance with the principles, legal limits, and rights of the Data Subjects, ensuring confidentiality, privacy, and secrecy of the transferred data in alignment with the provisions of the legislation.

6.6 Personal Data Storage, Retention, and Deletion

Personal Data will be retained for the period necessary to fulfill the work performed by TABOCA or for other legal purposes.

Subsequently, necessary measures will be taken for the deletion or anonymization of Personal Data, which can only be carried out in accordance with the guidelines established in this Policy. Personal Data maintained through manual or electronic records that have reached the retention date must be discarded as "confidential waste," removed from use, and destroyed immediately.

In the event of a request for deletion of Personal Data by the Data Subject, TABOCA reserves the right to retain such data in its Database to comply with legal obligations, resolve disputes, maintain security, prevent fraud, abuses, guarantee contract fulfillment, or provide information to public bodies, in which case the Personal Data must be anonymized.

6.7 Effectiveness and compliance

TABOCA will adopt all necessary means and actions to ensure compliance with this Policy, such as dissemination, adherence to terms of consent, contractual adjustments, training, disciplinary measures, and any other measures deemed necessary.

6.8 Contact

TABOCA has appointed Luiz Fellipe Salomão Queiroz as the Data Protection Officer to receive communications from Individuals and third parties, provide clarifications, and take appropriate measures, as well as to serve as a liaison with the National Data Protection Authority (ANPD).

To contact the Data Protection Officer, Individuals may send their requests to: E-mail: lgpdmtaboca@mtaboca.com.br

Luiz Fellipe Salomão Queiroz
Data Protection Officer (DPO)