

Whistleblowing and Social Concerns Policy

I. SCOPE, PURPOSE AND DEFINITIONS

Scope

1. This Policy applies to JP Sá Couto (jp.ik), JP Holding Services and Imotsu (the “companies”), as well as to all their employees, regardless of the nature of their contractual relationship, role or country in which they perform their activities, and to Third Parties with whom the companies have a business relationship (namely clients, suppliers and subcontractors).

2. In the countries where the companies operate, where the applicable legal and regulatory provisions on anti-corruption are less restrictive, the provisions set out in this Policy shall prevail, to the extent permitted by the relevant legal system.

3. More restrictive practices than those set out in this Policy may be implemented in countries where this is required under mandatory provisions of applicable law.

Purpose

1. This Policy aims to establish a set of rules governing:

a) the process for receiving, recording and handling reports of Infringements, in accordance with applicable legal provisions, as well as with the rules, principles and values set out in the Code of Ethics and Conduct and the Anti-Corruption and Related Offences Prevention Policy;

b) the process for receiving, recording and handling social concerns relevant to the SA8000 standard, relating to jp.ik or its business partners.

2. This Policy further aims to:

a) Define the concepts and establish the principles governing the reporting of infringements;

b) Identify reporting channels and define the respective procedures;

c) Establish the roles and responsibilities of those involved;

d) Promote employee awareness of their personal and professional duties in this matter and ensure compliance with the internal procedures in place.

3. For the purposes of this Policy:

I. Infringements

Infringements are acts or omissions, committed intentionally or negligently, as provided for and described in Article 2(1) of Law No. 93/2021 of 20 December and Article 3 of Decree-Law No. 109-E/2021, including but not limited to:

a) Corruption and related offences;

b) Environmental violations;

c) Breaches of privacy, personal data protection, and the security of networks and information systems;

d) Public procurement violations;

e) Consumer protection violations;

f) Anti-competitive practices;

g) Organised and financial-economic crime;

h) Harassment, whether physical or psychological;

i) Practices contrary to those set out in our Code of Ethics and Conduct.

II. Social Concerns

Social concerns include issues related to:

a) Child labour;

b) Forced labour;

c) Health and safety;

d) Freedom of association and collective bargaining;

e) Discrimination (including harassment practices);

f) Disciplinary practices;

g) Working hours;

h) Remuneration.

Any matter falling outside the scope defined above shall be redirected to the appropriate channels.

Definitions

For the purposes of interpreting and applying this Policy, the following definitions apply:

- a) Management: A person or group of people who direct and control the organisation at the highest level;
- b) Employee: Members of corporate bodies, managers, employees and trainees/interns;
- c) Code of Ethics and Conduct: A document comprising a set of principles governing the activities of the companies, and a set of ethical and professional rules to be observed by members of the corporate bodies and employees in their relationships with Clients, Suppliers and other Stakeholders. It also applies to third parties contracted by, or acting on behalf of, the companies, where the companies may be held responsible for their actions;
- d) Corruption: The offering, promising, giving, accepting or requesting of an undue advantage of any value (financial or non-financial), directly or indirectly, regardless of location, in violation of applicable laws, with the aim of inducing or rewarding a person for an action or omission in the performance of their duties or responsibilities;
- e) Related offences: Offences such as undue receipt or offer of advantage, embezzlement, economic participation in business, extortion, abuse of power, misconduct in office, influence peddling, money laundering, or fraud in obtaining or misusing subsidies, grants or credit;
- f) Unlawful act: Any act or omission, intentional or negligent, voluntary or involuntary, that violates any mandatory legal provision;
- g) Third Party: Any individual or legal entity who is not an employee but participates in activities promoted by the companies or has a business or similar relationship with them, including service providers, consultants or suppliers, directly or indirectly;
- h) Compliance Channel: An internal digital platform that enables, confidentially or anonymously, and ensuring the highest standards of information security, the submission of reports concerning unlawful acts, violations of our principles and values, and actual or potential adverse impacts on human rights, so that such acts may be investigated and, where appropriate, sanctioned;
- i) Report (Whistleblowing Report): A situation raised by a whistleblower regarding suspected or actual criminal conduct, unethical behaviour or other misconduct by the company(ies), or any of its employees, that leads or may lead to a violation of the Code of Ethics and Conduct, any policy, regulation, work instruction or other internal rules, and/or any legally binding law or regulation;
- j) Social Concern: A potential non-compliance situation, including concerns, questions, complaints, incidents and grievances relevant to the SA8000 standard;
- k) whistleblower / Complainant: Any natural person who reports or publicly discloses information on infringements or social concerns obtained in a work-related context;
- l) Business Partner Entity: An external entity with which the organisation has, or intends to establish, a business relationship;
- m) Interested Party: A person or organisation that can affect, be affected by, or perceive itself to be affected by a decision or activity;
- n) Business Partner: An entity with which the company maintains a business relationship to achieve its business objectives. This includes entities with which the organisation has direct or indirect relationships throughout its value chain, upstream and downstream, such as recruiters, recruitment agencies, suppliers, subcontractors, agents, licensees, intermediaries, distributors, service providers, and minority or majority interests in joint ventures;
- o) Retaliation: Any act or omission which, directly or indirectly, occurs in a work-related context and is motivated by an internal or external report or public disclosure, causing or potentially causing unjustified material or non-material damage to the whistleblower;
- p) Investigation: The investigation comprises the stages of assessing the admissibility of the report or social concern, establishing the grounds of the case, and, where appropriate, referring it to the competent investigation team(s);

- q) Anonymity: The identity of the whistleblower/complainant is unknown. A whistleblower is anonymous when their identity is not known to anyone (including those responsible for receiving reports and authorised persons);
- r) Authorised Persons: Individuals strictly authorised by the Compliance Officer. These include the Compliance Officer and the Legal Department. Management may be included on a case-by-case basis, taking into account potential conflicts of interest and confidentiality;
- s) Social Performance Team (SPT): A group composed of management and employee representatives, whose purpose is to support and facilitate the implementation of the social responsibility management system.

II. PRINCIPLES

Within the scope of this Policy, the following principles shall be observed:

- a) Independence and autonomy – procedures are adopted to ensure that the receipt, handling and storage of reports of irregularities are carried out in an independent, autonomous and impartial manner. All persons with a conflict of interest in relation to the matter reported shall be excluded from the assessment and decision-making process;
- b) Good faith and anonymity – all reports must be made in good faith and be adequately substantiated. The whistleblower may, if they so wish, request anonymity;
- c) Confidentiality and Data Protection – the confidentiality of received communications and the protection of personal data of both the whistleblower and the alleged offender are ensured, in accordance with applicable legislation. The anonymity of the whistleblower, the confidentiality of their identity and the details of the report are respected and protected.

III. ROLES AND RESPONSIBILITIES

Employees

Employees have a duty to promptly report any irregularity that has allegedly occurred, of which they are aware or which they can reasonably foresee may occur.

The Board

Management is responsible for:

- a) implementing, executing and overseeing this Policy, including establishing appropriate procedures for its compliance and ensuring that all employees receive adequate training;
- b) appointing a Compliance Channel Manager to ensure the proper handling of reports and social concerns received through the channel;
- c) ensuring the publication of, and access to, the Compliance Channel on the organisation's intranet and institutional website;

Compliance Officer

The Compliance Officer is responsible for:

- a) advising Management on the implementation of this Policy;
- b) carrying out first-line monitoring of the implementation and compliance with this Policy;
- c) advising Management on employee awareness initiatives (e.g. sharing best practices, training and communication materials);
- d) receiving reports and social concerns;
- e) ensuring the timely and appropriate follow-up of reported matters, in accordance with applicable laws and regulations, the Code of Ethics and Conduct, internal policies and procedures;
- f) providing the whistleblower with timely updates on the general progress of the investigation;
- g) promptly initiating the internal investigation process in cases where retaliation is reported;
- h) determining which individuals should be designated as Authorised Persons with access to the content of the report or social concern, ensuring that access is granted strictly on a need-to-know basis;
- i) providing, where applicable, information to other Authorised Persons on a strict need-to-know basis;

j) collecting annual metrics on reports and social concerns submitted through the Compliance Channel.

IV. PROCESS FOR HANDLING REPORTS AND SOCIAL CONCERNS

1. Reports and social concerns shall be promptly investigated, recorded and maintained in accordance with applicable laws, regulations, policies and procedures.
2. There are several ways to report a concern or submit a report:
 - a) Contacting the relevant line manager within the company;
 - b) Contacting the Compliance Officer;
 - c) In the case of social concerns, contacting the employees' representative for SA8000;
 - d) Submitting an anonymous or confidential message through the [Compliance Channel](#);
 - e) Reporting through the external channel maintained by the competent authority.

Internal procedure specific to social concerns

Where a social concern is reported to a line manager or to the employees' SA8000 representative, they must:

- Receive the communication impartially;
- Inform the Social Performance Team (SPT);
- Ensure the confidentiality of both the information and the reporting individual.

Where the matter corresponds to a query, clarification or a simple issue capable of immediate and consensual resolution, the line manager or SA8000 representative may:

- Forward the matter directly to the People Department or another competent area;
- Monitor the resolution of the matter;
- Where the issue is resolved but requires a corrective or improvement action, inform the Compliance Officer, who shall record it under the Corrective Actions and Improvement procedure.

Where the matter is not resolved, or where its nature, severity or impact justifies it, the communication shall be forwarded to the Compliance Officer in accordance with Annex III of this Policy.

Investigation Process

1. All reports and social concerns received shall be handled confidentially.
2. In order to ensure independence, impartiality, confidentiality, data protection, secrecy and the absence of conflicts of interest, the Compliance Channel is administered by WhistleB, an external service provider.
3. All messages are encrypted. To ensure anonymity, WhistleB removes all metadata, including IP addresses. The reporting individual may remain anonymous in any subsequent dialogue with those responsible for handling the report.
4. Access to reports and social concerns submitted through the Compliance Channel is restricted to the investigation team.
5. The investigation team consists of:
 - a) the Compliance Officer;
 - b) the Legal Team;
6. Where necessary, individuals with specialised knowledge may be involved in the investigation process.

Reports (Whistleblowing Reports)

Within seven days of receipt, the whistleblower shall be notified of the receipt of the report and informed, in a clear and accessible manner, of the requirements, competent authorities and procedures for external reporting, in accordance with legal provisions.

Reports shall be rejected where one of the following circumstances applies:

- a) Lack of substantiation;
- b) Submission in bad faith or malicious intent;
- c) Insufficient information to allow further investigation;
- d) The matter has already been resolved.

Following receipt of a report, the investigation team shall take appropriate internal steps to verify the allegations, documenting and recording the facts and circumstances established, including evidence

gathered, with a view to preparing a report on whether the report is substantiated and any measures to be adopted.

Feedback on the report shall be provided to the whistleblower within a maximum period of three months from the date of receipt.

Upon completion of the investigation, the whistleblower shall be informed, with appropriate justification, of:

- a) Whether the report was substantiated;
- b) The conclusions of the investigation;
- c) Where applicable, the measures taken and the rationale for such measures.

The whistleblower may incur disciplinary and/or criminal liability in the event of a false report made intentionally and/or in bad faith.

Where, as a result of the investigation, the report indicates the existence of a criminal offence, the Compliance Officer shall report the matter to the competent authority. In such cases, the whistleblower shall also be informed of all actions taken up to that point.

Social Concerns

14. Upon receipt of a social concern, the investigation team shall analyse the available information and conduct the investigation in a discreet and impartial manner, involving the SPT and Management, ensuring the absence of conflicts of interest.

15. The investigation team shall take appropriate internal steps to verify the allegations, documenting and recording the facts and circumstances established, including evidence gathered, with a view to preparing a report on whether the concern is substantiated and any measures to be adopted.

16. Based on the evidence collected, the investigation team, in collaboration with the SPT, shall determine whether the concern is substantiated and, where non-compliance is confirmed, define corrective and mitigation actions to eliminate the issue and prevent recurrence.

17. Feedback on the social concern shall be provided to the complainant within a maximum period of one month from the date of receipt.

Personal Data Processing

1. The Personal Data Protection Policy in force within the companies shall apply.

2. The companies are responsible for the personal data processed within the whistleblowing service.

3. For this purpose, WhistleB Whistleblowing Centre AB (World Trade Centre, Klarabergsviadukten 70, SE-107 24, Stockholm) is engaged as the provider of the reporting channel, including the processing of encrypted data such as messages. Neither WhistleB nor any of its sub-processors can decrypt or read messages. Accordingly, neither WhistleB nor its sub-processors have access to readable content.

Archiving and Retention

Reports and social concerns are stored within the Compliance Channel. Records of reports and social concerns, in anonymised form, shall be retained for a minimum period of five (5) years and, regardless of this period, for the duration of any judicial, administrative or disciplinary proceedings arising from the report, as required by law.

V. MANAGEMENT SYSTEM

Where a social concern is found to be substantiated, it shall be recorded under the Corrective Actions and Improvement procedure, and corrective actions shall be defined and implemented to eliminate the causes of the occurrence and prevent recurrence, with their effectiveness subsequently assessed.

The results, trends and learnings arising from reports and social concerns handled under this Policy shall be analysed with Management and considered within management review processes, contributing to the continuous improvement of the management system.

VI. FINAL PROVISIONS

Publication and Entry into Force

This Policy shall enter into force immediately upon its approval and shall be reviewed every three (3) years, or whenever deemed necessary. It shall be published on jp.hub and on the official website of the companies within ten (10) days of its implementation and/or revision.

ANNEX I

EXCEPTIONS TO THE PRINCIPLE OF CONFIDENTIALITY

Identity

As a general rule, the identity of a whistleblower/complainant who has not reported anonymously is known only to the individual receiving the report or social concern and to the members of the investigation team assigned to handle the case, and shall not be disclosed to any other person, except where:

- it is strictly necessary for one or more Authorised Persons to be aware of the identity, and only with the prior consent of the whistleblower; and/or
- there is a legal obligation to disclose the identity of the whistleblower/complainant.

Legal Obligation

An exception to the principle of confidentiality shall apply where there is an obligation under applicable law or regulation to disclose information relating to a report or social concern to an external party that is duly authorised, including, without limitation, in response to court orders, requests from public authorities, law enforcement bodies, or similar entities.

Where the Companies Decide to Report

An exception to the principle of confidentiality shall also apply where the content of the report or social concern, or the outcome of subsequent procedures, requires disclosure of information to competent authorities.

In such cases, the confidentiality of the identity of the whistleblower/complainant shall be respected, unless there is a legal obligation to disclose it. The whistleblower/complainant shall be informed in advance.

ANNEX II

REPORTS RELATING TO MANAGEMENT AND/OR THE COMPLIANCE OFFICER

Reports relating to the Board

Where a report relates to a member of the Board, the whistleblower shall submit the report directly through the internal reporting channel, thereby ensuring full follow-up of the matter.

Following a preliminary investigation and where the allegations are found to have serious grounds, the Compliance Officer shall refer the report for external investigation.

Reports relating to the Compliance Officer or DPO

Where a report relates to the Compliance Officer, the whistleblower shall communicate the concern directly to the People Department, which shall refer the matter for a full investigation by external investigators.

Where a report relates to the People Department, the whistleblower shall submit the report directly through the internal reporting channel, and a full investigation shall be carried out.

Where a report relates to the DPO, the whistleblower shall submit the report directly through the internal reporting channel, and a full investigation shall be carried out.

ANNEX III

REPORTS OR SOCIAL CONCERNS SUBMITTED IN PERSON OR BY EMAIL

I. Where a report or social concern is submitted in person to the Compliance Officer, the Compliance Officer shall prepare a complete and accurate written record of the report or concern, the content of which shall be confirmed and validated by the whistleblower/complainant.

II. Where a report or social concern is submitted by email to the Compliance Officer, the Compliance Officer shall prepare a complete and accurate written record of the report or concern.

III. Where a report or social concern is submitted to a line manager, the latter must forward it to the Compliance Officer within a maximum of one (1) working day from receipt, who shall ensure the procedure referred to in point II above.

IV. Where a social concern is submitted to the employees' SA8000 representative, the latter must forward the information to the Compliance Officer within a maximum of one (1) working day from receipt, who shall ensure the procedure referred to in point II above. In this case, the employees' representative shall accompany the investigation and resolution process, ensuring confidentiality throughout.

ANNEX IV

INDICATIONS, SUSPICIONS AND RUMOURS

Any indication, suspicion, rumour or mere awareness of a potentially suspicious act relating to criminal conduct, unethical behaviour or other misconduct, including violations of the Code of Ethics and Conduct, any internal policy or regulation, and/or any legally binding law or regulation, shall be promptly investigated in accordance with the provisions set out in this Policy.