WHISTLEBLOWING POLICY

jp.group has implemented this Policy for the purpose of establishing a series of internal rules and procedures for the receipt, recording and processing of reports of Offences, in accordance with the applicable legal provisions, as well as the rules, principles and values outlined in the Group's Code of Ethics and Conduct and the Policy for the Prevention of Corruption and Related Offences.

1. Object and Scope

1.1. The objectives of this Policy are as follows:
a) Defining applicable concepts and establishing the principles that govern the reporting of offences;
b) Identifying whistleblowing channels and defining the respective procedures;
c) Establishing the roles and responsibilities of the individuals involved;
d) Contributing to raising employee awareness of their personal and professional duties concerning these matters and emphasising the importance of ensuring compliance with the internal procedures in place.

1.2. This Policy is applicable to all jp.group companies located in Portugal, as well as all employees and any Third Parties with which jp.group engages in business relationships (namely clients and suppliers). In jurisdictions where (local) laws or regulations establish more stringent rules than those outlined in this Policy, the former shall prevail.

1.3. For the purposes of this Policy, an Offence is defined as any of the intentional or negligent acts or omissions outlined and described in Article 2, paragraph 1, of Law no. 93/2021, of 20 December, as well as Article 3 of Decree Law No. 109-E/2021, including but not limited to the following:
a) Corrupt practices and related offences;
b) Health and safety violations;
c) Environmental violations;
d) Violations of privacy, personal data and network and information system security;
e) Public procurement;
f) Protection against radiation and nuclear safety;
g) Consumer protection;
h) Practices that distort competition;
i) Organised and economic-financial crime;
j) Practices of physical or moral harassment;
k) Discriminatory practices;
l) Practices contrary to sustainability, as listed in the Code of Ethics and Conduct.

2. Definitions

For the purposes of this Policy, the following definitions shall apply:
a) jp.group: the group of companies owned and held, directly and/or indirectly, by JP Holding Services, S.A.;
b) Employees: members of the governing bodies, managers, workers and trainees;
c) Senior Management: Appointed persons who are individually or jointly responsible for decision-making, general operation, and administration of legal entities, business lines, departments and management bodies or similar entities;
d) Code of Ethics and Conduct: a document that outlines a series of principles that govern the activity of the companies that comprise jp.group, as well as a set of ethical and deontological rules to be observed by the members of the respective Governing Bodies and all Employees in their relationships with Clients, Suppliers and other Stakeholders. It is also intended for third parties contracted or acting on behalf of jp.group companies, particularly in situations where the actions of the former could lead to accountability for the latter;

e) Corruption and related offences: the crimes of corruption, undue receipt and offering of advantages, embezzlement, economic participation in business, extortion, abuse of power, prevarication, influence peddling, money laundering or fraud in obtaining or diverting subsidies, grants or credit;
f) Unlawful act: any intentional or negligent act or omission, voluntary or involuntary, that violates any imperative legal provision;
g) Third party: any natural or legal person not employed by jp.group that participates in activities promoted by the Group, or has a commercial or similar relationship with the latter, as a service provider, consultant or supplier of goods or services, directly or indirectly;
h) Internal whistleblowing channel: an internal digital platform provided for the submission of reports concerning the commission of unlawful acts or violations of the principles and values or jp.group, in a confidential or anonymous manner, ensuring the highest standards of information security, such as to allow the investigation and sanctioning of such acts, if justified;
i) Report: a situation raised by a whistleblower concerning a suspected or actual criminal conduct, unethical behaviour or any other misconduct by jp.group, or any of its employees, that leads or may lead to a violation of the Code of Ethics and Conduct, any jp.group policy or regulation and/or any legally binding law or regulation;
j) Whistleblower: any individual who reports or publicly discloses information about violations, obtained in a professional context;
k) Retaliation: any act or omission occurring in a professional context, motivated by an internal or external report or public disclosure, that causes or may cause, directly or indirectly, unjustified material or non-material losses to the whistleblower;
l) Investigation: an investigation consists of two stages: Preliminary Investigation and Full Investigation. The first stage is conducted by the Operator/Channel Manager and involves the assessment of the admissibility of the report, the examination of the respective grounds, and its forwarding to the competent investigative team(s), such as to allow the investigation of the reported situation. The second stage will be conducted by the relevant investigative unit and/or any external party appointed by the competent unit, in accordance with the applicable policies and procedures;
m) Anonymity: the identity of the whistleblower is unknown. A whistleblower is anonymous when their identity is not known to any employee (including the employees responsible for receiving reports at jp.group and authorised persons);
n) Authorised Persons: the individuals considered strictly necessary for the follow-up and/or investigation of the whistleblower's concern. The Channel Operator selects the individuals who qualify as/ become Authorised Persons. The Authorised Persons include the Whistleblowing Channel Operator (systematic), the Regulatory Compliance Officer and the Legal Department. The Management may be included in the group of Authorised Persons; however, this must be determined by the internal Whistleblowing Channel Manager on a case-by-case basis, taking potential conflicts of interest and confidentiality into special consideration.
o) Channel Operator: employee appointed to manage the receipt and processing of reports submitted through the internal whistleblowing channel.

3. Principles

The following principles should be observed within the scope of this Policy:
a) Independence and autonomy - jp.group has implemented procedures aimed at ensuring that irregularities are received, processed and archived in an independent, autonomous and impartial manner, and that all individuals with conflicting interests in the reported matters are excluded from the investigation and decision-making process;
b) Good faith and anonymity - all reports should be submitted in good faith and be based on adequate grounds. Whistleblowers may request to remain anonymous should they wish to do so;
c) Confidentiality and Data Protection - jp.group ensures the confidentiality of the reports received and the protection of the personal data of the whistleblower and the suspected perpetrator, in accordance with the applicable legislation. The anonymity of the whistleblower, the confidentiality of their identity and the details of the report are respected and protected. Please refer to Annex I for exceptions to the principle of confidentiality. The data of the whistleblower and/or data subjects involved in investigations are adequately recorded and/or retained and destroyed in accordance with the applicable laws, regulations, policies and procedures.
d) Non-retaliation - jp.group is not allowed to terminate, threaten, suspend, repress, harass, withhold or suspend any salary payments and/or benefits, or take any retaliatory action against any individual who reports an irregularity in a lawful manner.

4. Roles and Responsibilities

4.1. Employees
The employees have the duty to immediately report any alleged irregularity of which they become aware or whose occurrence can reasonably be foreseen.

4.2. Management
Without prejudice to the provisions included in paragraph 1, the Management is responsible for:
a) implementing, carrying out and monitoring this Policy, including the establishment of adequate procedures for ensuring compliance therewith and the provision of suitable training to all employees;
b) appointing a channel manager to ensure the adequate management of reports received through the internal whistleblowing channel;
c) ensuring that the internal whistleblowing channel is published and accessible on the Organisation's intranet and institutional website;

4.3. Regulatory Compliance Officer
Without prejudice to the provisions included in paragraph 1, the Regulatory Compliance Officer is responsible for the following:
a) advising the Board of Directors and Senior Management on the implementation of this Policy;
b) conducting first-line monitoring of the implementation and compliance with this Policy;
c) promoting regular audits of the internal whistleblowing system;
d) establishing procedures for the receipt, retention and processing of reports received by jp.group in the context of audits.

4.4. Channel Operator
The Channel Operator is responsible for the following:
a) receiving reports and providing acknowledgments of their receipt to whistleblowers;
b) processing the reports received in a timely, adequate manner, in compliance with the applicable laws, the Code of Ethics and Conduct and the relevant policies and regulations of jp.group;
c) conducting investigations whenever the situations reported fall within the scope of the regulatory compliance programme;
d) consulting the Regulatory Compliance Officer: I. whenever the Management is the subject of the report; II. if retaliation is reported;
e) providing timely updates on the overall progress of the investigation to whistleblowers;
f) immediately initiating the internal investigation process if retaliation is reported;
g) selecting the Authorised Persons, i.e. individuals allowed to access the contents of the report. Access should only be authorised when strictly necessary for processing and/or investigation purposes;
h) providing information to the Regulatory Compliance Officer and other authorised persons, on a strict "need-to-know" basis;
i) collecting annual metrics of concerns reported through the internal whistleblowing channel of jp.group.

5. Report Processing

5.1. Report
5.1.1 Reports are promptly investigated, recorded and maintained in accordance with the applicable laws, regulations, policies and procedures.
5.1.2 Reports can be submitted through any of the following means:
a) Contacting a hierarchical superior within the organisation;
b) Contacting the Regulatory Compliance Programme Manager;
c) Sending an anonymous or confidential message to the whistleblowing team through the whistleblowing channel: https://report.whistleb.com/jphs
d) Communication to the external channel maintained by the competent authority.

5.2 Investigation process

5.2.1 All reports received will be treated confidentially.

5.2.2 The whistleblowing channel is managed by WhistleB, an external service provider, in order to ensure independence, impartiality, confidentiality, data protection, secrecy and the absence of conflicts of interest in the performance of duties.

5.2.3 All messages are encrypted. WhistleB removes all metadata, including IP addresses, in order to protect the anonymity of the senders. Senders will also remain anonymous, should they wish, in the subsequent dialogue with report recipients.

5.2.4 Access to messages received through the whistleblowing channel is restricted to the whistleblowing team.

5.2.5 The whistleblowing team consists of the following:

a) Regulatory Compliance Officer;

b) People Management;

c) External channel operator (inCentea).

5.2.6 Specialists may be called to participate in the investigative process, whenever required.

5.2.7 The whistleblower will be notified of receipt of their report within 7 days from the respective reception date. Additionally, the whistleblower will be informed, in a clear, accessible manner, of the requirements, competent authorities, and form and admissibility of external reports, in accordance with the law.

5.2.8 Reports will be rejected if any of the following circumstances apply:

a) Lack of grounds;

b) Reports submitted in bad faith or malicious;

c) Insufficient information to allow further investigation;

d) The matter has already been resolved.

5.2.9 After receiving the report, the whistleblowing team will follow the necessary steps to verify the allegations contained therein, ensuring that the facts and circumstances investigated, including the evidence produced, are adequately recorded, such as to enable the production of a report on the validity of the submitted information and any measures to be eventually adopted.

5.2.10. The whistleblower will be informed of the steps taken to follow up on the report within three months from the respective date of receipt.

5.2.11. Upon completion of the investigation process, the whistleblower will be informed of the following:

a) If the report was considered valid;

b) The conclusions reached with respect to the report; c) If applicable, the measures taken to follow up on the report and the respective grounds.

5.3 Processing of Personal Data

5.3.1 The Personal Data Processing Policy of jp.group applies.

5.3.2 Jp.group companies are responsible for the personal data processed within the scope of the whistleblowing service.

5.3.3 WhistleB Whistleblowing Centre Ab (World Trade Centre, Klarabergsviadukten 70, SE-107 24, Stockholm) has been subcontracted to provide and manage the whistleblowing channel, including the processing of encrypted data, such as report messages. Neither WhistleB nor any subcontractors are allowed to decrypt and read messages. Therefore, neither WhistleB nor its subcontractors have access to readable content.

6. Publication and Effectiveness

This Policy shall come into effect immediately after its approval and will be reviewed every 3 years, or whenever justified. The Policy will be published on jp.hub and the official website of jp.group within 10 (ten) days of the respective implementation and/or revision.

7. Reference to other documents

Data Processing Policy	The Personal Data Processing Policy establishes the principles that employees and third parties are required to follow with respect to the collection, use, retention, transfer, disclosure and destruction of data of natural persons, in what regards the processing and free movement of Personal Data.
Policy for the Prevention of Corruption and Related Offences	The Anti-Corruption Policy aims to implement the principles of action and duties outlined in the jp.group Code of Ethics and Conduct, with respect to honesty and integrity. This Policy establishes guidelines to prevent unlawful conducts that constitute acts of corruption and potential conflicts of interest.
Whistleblowing Channel FAQs	The Internal Whistleblowing Channel FAQs are intended to provide clarification on the terms and requirements associated with the use of the jp.group internal whistleblowing channel.
Manual of Internal Investigation Methods and Procedures	The Manual of Internal Investigation Methods and Procedures aims to establish a standardised internal procedure for investigating situations reported through the whistleblowing channels of jp.group.
Case Management Process	The Case Management Process aims to provide guidance to all individuals responsible for receiving reports through the jp.group whistleblowing channel with respect to the correct use of the platform and the required precautions concerning reports, report processing and the personal data stored on the platform.

Annex I – Exceptions to the confidentiality principle and External Whistleblowing Channels

All individuals retain the right to disclose relevant information to the competent authorities, irrespective of the obligation to uphold the confidentiality principle. However, precedence rules between reporting channels dictate that the whistleblower can only resort to external reporting channels in the following situations:

- No internal whistleblowing channel is available;
- The internal whistleblowing channel only allows the submission of reports by workers, not by the whistleblower;
- The whistleblower has reasonable grounds to believe that the offence cannot be effectively known or resolved internally, or that a risk of retaliation exists;
- The whistleblower initially submitted an internal report, but failed to receive information on the measures envisaged or adopted within the legally specified deadlines; or
- The offence constitutes a crime or infringement punishable with a fine exceeding €50,000. Any whistleblower who submits an external report without observing the precedence rules applicable to the whistleblowing channels available shall not be entitled to the protection afforded by law, unless, at the time of submission, they were unaware of the aforementioned rules, through no fault of their own.

Exceptions to the confidentiality principle:

1. Identity

As a matter of principle, the identity of any whistleblower who has not submitted a report anonymously is only known to the jp.group Channel Manager receiving the report and the members of the investigative team assigned to follow up on the matter. The identity of the whistleblower will not be disclosed to any other individual, except in the following situations:

- If disclosure to one or more authorised persons is strictly necessary, after the prior consent of the whistleblower is obtained; and/or
- jp.group is legally obligated to disclose the identity of a whistleblower.

Exceptions to the confidentiality principle:

1. Identity
As a matter of principle, the identity of any whistleblower who has not submitted a report anonymously is only known to the jp.group Channel Manager receiving the report and the members of the investigative team assigned to follow up on the matter. The identity of the whistleblower will not be disclosed to any other individual, except in the following situations:
- If disclosure to one or more authorised persons is strictly necessary, after the prior consent of the whistleblower is obtained; and/or
- jp.group is legally obligated to disclose the identity of a whistleblower.

2. Legal obligation
An exception to the confidentiality principle arises when jp.group is obligated by law, or any applicable regulation, to disclose information regarding a specific report to an external party, duly authorised to request and receive such information.

3. When jp.group decides to report
An exception to the confidentiality principle arises when jp.group decides that the content of the report or the outcome of the subsequent proceedings entail the disclosure of information to the competent authorities. Should jp.group opt for sharing details with the competent authorities, the identity of the whistleblower will be kept confidential, unless jp.group is legally obligated to disclose this information.

Annex II – Reports concerning the Management, individuals responsible for receiving internal reports and the Channel Operator or Regulatory

Reports concerning the Board of Directors or Senior Management

If a member of the Board of Directors or Senior Management of jp.group is concerned, the whistleblower should submit the report directly to the internal whistleblowing channel, such as to ensure that the situation will be meticulously investigated. Following a preliminary investigation and confirmation that the allegations are based on solid grounds, the Channel Operator shall forward the report to the Regulatory Compliance Officer, who will refer the report for external investigation.

Reports concerning the person Responsible for receiving reports, the Regulatory Compliance Officer or the DPO

If the Regulatory Compliance Officer is concerned, the whistleblower should submit the report through the internal whistleblowing channel. The Channel Operator will forward the report for full investigation by external investigators.

If the Channel Operator is concerned, the whistleblower should submit the report directly to the Regulatory Compliance Officer. The latter will initiate a full investigation of the report through the email address etica@groupjp.com, or in person.

If the DPO is concerned, the whistleblower should submit the report directly to the Regulatory Compliance Officer. The latter will initiate a full investigation of the report through the email address etica@groupjp.com, or in person.