PARTECH

WHISTLEBLOWING

POLICY

2023

¶

Document Reference Code		PP01-03		
Name		Whistleblowing Policy		
Document Owner		Compliance & Risk		
Reviewer		Excom		
Approver(s)		Excom		
Document Access Permissions:				Company-wide
French translation available				No
Effective from Date		10/2023	Review Cycle	Annually
Version no.	Draft Date	Author	Approval Date	Comments
1	09/2023	Compliance & Risk	19/10/2023	Creation

TABLE OF CONTENTS

¶

I. GENERAL PROVISIONS

1. Context

Partech is committed to maintaining a transparent, ethical, and responsible work environment where all employees and third parties are encouraged to report concerns, wrongdoing, or unethical behavior without fear of retaliation. It is then important for Partech to have clear procedures and policies in place regarding whistleblowing.

By promoting a culture of openness and accountability, Partech strives to maintain the highest standards of ethical conduct, integrity, and professionalism.

2. Purpose

This Policy complements the provisions of Partech's Code of Conduct that set forth a corpus of ethical rules applicable to Partech and Partech Employees for the day-to-day operations and particularly with respect to the conduct of business in a professional, fair, honest, and ethical manner.

The purpose of this policy is to establish clear guidelines for reporting concerns, outline the steps that should be taken to investigate those concerns and provide safeguards to protect the rights and confidentiality of whistleblowers.

This policy applies to all employees, contractors, consultants, and any other individuals associated with Partech.

II. WHISTLEBLOWING PROCESS

1. General principles

A whistleblower (the "Whistleblower") is any person falling into a category below:

- any staff member who is a permanent or temporary employee e.g., full-time, part-time, secondees, interns or alternants,
- any suppliers (including its employees), freelancers, subcontractors,
- any third party related to Partech such as investors, business service providers etc.

The Whistleblower must act selflessly and in good faith.

The Whistleblower is a person who reveals or reports, selflessly and in good faith, a crime or an offense, a clear and serious violation of a commitment, a law or regulation, or a threat or harm to general interest that he/she knew about personally.

Whistleblowers must have personally become aware of the facts reported.

In case the individual has not become personally aware of the facts reported or has been told the fact by another person or based on a suspicion or an unsubstantiated allegation, the reported facts will be considered invalid. The Whistleblower should not in any case try to conduct his/her own investigation.

2. Activities covered by the whistleblowing protection

The subject of the report may be any crime or offense, any serious and clear violation of rules and regulations, a law or an international treaty, or any serious threat or damage to the general interest.

To illustrate, the report may relate to any fact or conduct constituting a violation of the rules regarding:

- any violation of regulation and/or law (national or international),
- breach of professional and ethics rules,
- infringements of the rules for the protection of client's interests,
- leakage of confidential information,
- inappropriate or unprofessional behavior towards employees, including sexual and moral harassment, discrimination,
- acts of fraud, embezzlement, and theft,
- acts of corruption,
- violation of regulation or laws or internal procedures,

- acts of fraud, negligence, breach of trust or duty,
- violation of human rights,
- any damage to the health and/or safety of persons or the environment noticed within activities performed by the portfolio companies in which the managed Funds invest or, by suppliers,
- financial crimes (sanctions, embargoes, market abuse).

The Whistleblower of the alert's protection does not cover facts, information, or documents in whatever form or on whatever medium they may be when those facts, information, or documents are classified as "Secret-Défense" or covered by medical confidentiality or client-attorney privilege.

3. Reporting of facts

Persons within the scope of the Policy may report the matter to the Chief Compliance & Risk Officer or the Head of HR or, by sending an email to securespeak@partechpartners.com.

The examination and processing of the reports are carried out by Partech in complete confidentiality.
The report must be factual and should not be speculative. It should contain any relevant information or documents supporting the reported facts to allow a proper assessment of the nature and the extent of the concern.
It should be as exhaustive, accurate, and detailed as possible.
The Whistleblower is invited to provide his/her contact details information (name, surname, contact details) for follow-up correspondence.
An acknowledgment of receipt will be promptly sent to the Whistleblower by email and within a maximum period of 3 months, the Whistleblower will be informed by email that remediation actions have been taken, where applicable.

4. Confidentiality

Partech undertakes to keep such information confidential.

Whistleblowers' identities and the identity of the persons who supported a Whistleblower shall not be revealed to the person concerned by the investigation or to any other person, in the absence of strict need-to-know or legal grounds, unless:

- the Whistleblower authorizes in writing the disclosure of his or her identity; or
- this is a necessary and proportionate requirement in the context of the investigations conducted by the competent services and authorities; or
- this is a requirement in any subsequent legal proceedings; or
- Partech has otherwise a legal obligation to disclose such information, including in the context of subsequent disciplinary proceedings.

5. Protection against retaliation

Where a Whistleblower, a person who has supported a Whistleblower or a person associated with a Whistleblower reasonably believes she/he is threatened with retaliation or retaliated against because she/he reported information, the Chief of Compliance & Risk shall provide appropriate assistance to secure his/her protection.
Should the retaliation or the threatened retaliation come from the Chief of Compliance & Risk, the Head of HR shall provide appropriate assistance to secure the Whistleblower's protection.

Any misuse of the mechanism by false reports (notification of information known to be totally or partially inaccurate) or acting in bad faith makes the Whistleblower liable to the prosecution provided by law and, in accordance with the Internal Regulations, to disciplinary sanctions.

Any employee hindering or having hindered the submission of a report or having engaged in retaliation against a Whistleblower may be subject to prosecution and may also face disciplinary sanctions, in accordance with the "Partech's Réglement Intérieur".

III. PROCESSING OF THE ALERT

1. Whistleblowing Referents

The referent receives and analyzes the reports submitted.

The Referents are the Chief Compliance & Risk Officer and the Head of HR unless there is a clear conflict of interest. In this case, the Executive Committee (ExCom) will authorize and appoint an independent person to investigate.

In conjunction with the members of Partech's ExCom, the Referents ensure the absence of conflict of interest by any member involved in an investigation and ensure the replacement of the Referent (and his/her representative) where needed.

2. Alert procedure

In handling a report, the Referents may require the support of internal teams or external advisors.
The Referents must be independent and unbiased.

Partech aims at handling the report as follows:

- examination of the admissibility of the report will be carried out within fifteen (15) business days following receipt of the report. The Whistleblower shall be informed of the decision.
- If the report is admissible, an investigation will be carried out within three (3) months maximum. However, in exceptional circumstances, the timeframe of such investigation may be extended.
- If needed, a general update without specific details may be provided to the Whistleblower during the investigation phase.
- At the end of the investigation, the Referents and/or the representatives will provide the Executive Committee with a report including:
    - Recommendations (to close the investigation without any action, launch a disciplinary process, inform the authorities, etc.).
    - An action plan for remediation if needed.
    - The possible disciplinary sanctions to be imposed on a Whistleblower in the event of a report made in bad faith.

Information on the general outcome and closure report will be provided to the Whistleblower.

The Referents and his/her representatives shall update on a regular basis the Executive Committee if required.

3. Processing of personal data

The Referents, as the person responsible for processing, take all precautions needed to ensure the security and integrity of the collected data, both at the time of collection and processing of the data and at the time of communication for investigation purposes and recordkeeping after the case is closed.

IV. ALTERNATIVE EXTERNAL REPORTING CHANNELS

The author of the alert is not permitted to release the alert to the public, unless no action is taken by the Referents. In this case, the alert is addressed to the judicial or administrative authority or the relevant professional order.

In case of serious and imminent danger or possible irreversible damages, the alert may be addressed directly to the judicial or administrative authority or the relevant professional order.

The alert can also be addressed to the French financial authority ("Autorité des marchés financiers") using the following address: lanceurdalerte@amf-france.org or by mail marked "Confidential" to the following address:

AMF Division de la Surveillance des marchés
17, Place de la Bourse.
75082 Paris Cedex 02.

The AMF can also be reached by phone on the following number: +33 1 53 45 64 44.

Also, if no diligence is taken by the judicial or administrative authority or the relevant professional order within three months of receipt of the alert, the alert can be made available to the public.

In addition, every person can address her/his alert to the Commissioner for Human Rights ("Défenseur des droits") to be geared toward the body to whom the alert should be sent.

The alerts received are submitted to an automatic processing authorized by the "Commission nationale de l'informatique et des libertés" (C.N.I.L.).

Under the "Sapin II" law, an employer cannot take adverse action against the author of the alert when this person is an employee, such as firing or laying off, demoting, failure to hire or rehire, intimidation or harassment, etc.