Fortidia

Global Whistleblowing Policy

Effective Date: December 15, 2023

1. PURPOSE

Our success as an organization is built on a foundation of ethical decision-making and a commitment by every employee to uphold the highest standards of professional conduct on the job. The best way to sustain an ethical culture is for each of us to act with integrity every day - doing the right thing when it comes to our own behavior, being aware of what's going on around us and being willing to speak up when we see or suspect activity that could harm us and our organization.

The purpose of this Whistleblowing Policy (hereinafter the **Policy**) is to provide People with support and guidelines to speak up and report any potential, or actual, unethical, unlawful, unsafe or discriminatory conduct, which violates any law, regulation or MBE Group or local policy, without risking to be subject to retaliation. This conduct can take many forms, such as malpractice, corruption, harassment, fraud, or negligence.

For the purpose of this document the following definitions apply:

- **Breach**: any act or omission that constitutes a breach of any laws, regulations or MBE policies.
- **Misconduct**: any act or omission occurred or most likely to occur in our organization which triggers a Breach and which is considered as harmful to the organization, its People and even the public interest.
- **MBE Group**: means any existing legal entities directly or indirectly controlled by MBE Worldwide S.p.A.
- **People**: means any of the following:
    - employees, including paid or unpaid trainees/students, and volunteers,
    - self-employed persons providing services, consultants, freelance workers, contractors, subcontractors and suppliers,
    - candidates involved in recruiting processes for any company of the Group;
    - persons whose work-based relationship with the Group has ended;
    - shareholders and or persons exercising (directly or indirectly) any administrative, management, supervisory or representative function with MBE Group; and
    - any other persons who are/have been in a Work-Related Context with one of the companies belonging to the MBE Group;
- **Person Concerned:** means a natural or legal person who is referred to in a Report as someone to whom a Breach is attributed or with whom a Breach is associated.
- **Report**: means the oral or written communication of information relating to any Breach.
- **Reporting Person**: any individual who files any Report(s) through the Whistleblowing Channels.
- **Receiving Person**: the Direct Manager or People Manager to whom the Reporting Person issues the Report using the Direct Channel.
- **Whistleblowing Channels**: means the tools and systems implemented and organized by MBE Group for ensuring compliance with Whistleblowing Regulation.

- **Whistleblowing Regulation** means the whistleblowing EU legislation and any local whistleblowing legislation, where applicable to MBE Group.
- **Work-Related Context**: means any current or past work activities through or in the context of which, irrespective of their nature, a person may acquire information on Breaches.

2. ELIGIBILITY

The principles set out in this Policy apply to all People.
People have a duty to be aware of the contents of this Policy and any updates, and to comply therewith.
This Policy will be published on the People Center, other local intranet and the public website MBECorporate.com.

3. AIM & SCOPE

This Policy aims to:

- encourage People to feel confident in raising all Reports made in good faith;
- provide avenues for People to raise Reports and receive feedback on any action taken;
- ensure that People receive a response to their Reports and that they are aware of how to pursue further steps if they are not satisfied with any response; and
- reassure People that they are protected for reporting in good faith, with no risk of direct or indirect retaliation.

4. SAFEGUARDS & OBLIGATIONS

Harassment or victimization
The MBE Group is committed to good practice and high standards and supporting its People. The MBE Group will not tolerate any harassment or victimization (including informal pressures) that occurs as a result of a member of staff seeking to raise such concerns; and, it will take appropriate action to protect staff when they raise a concern in good faith. Any investigation into allegations of potential malfeasance will not influence or be influenced by any disciplinary or redundancy procedures that already affect an employee or that may be under way in relation to them.

To enjoy protection, Reporting Persons must act in good faith, meaning that they reasonably believe or suspect, considering the circumstances and the information available to them at the time of reporting, that there has been a breach or violation of any laws, regulations, or MBE Group or local policies. This requirement is an essential safeguard against malicious or abusive reports: those who deliberately and knowingly report wrong or misleading information do not enjoy protection.

Confidentiality and Anonymity
All Reports will be treated as confidential and every effort will be made to protect the anonymity of People involved if they so wish. The organization is prohibited from further investigating the identity of the Reporting Person or taking any action on retaliation against the Reporting Person where the

Reporting Person has provided information anonymously.

This Policy encourages People to put their name on their allegation whenever possible, because it can be difficult or even impossible to investigate a Report without obtaining further information from the Reporting Person.

Data Protection

In the management of the Whistleblowing Channels, the processing of personal data must comply with the GDPR and any applicable local data protection legislations.
MBE Group identifies technical and organizational measures suitable to guarantee a level of security appropriate to the specific risks arising from the relevant processing of personal data, based on a data protection impact assessment. In compliance with the minimization principle, MBE Group does not collect or, if collected, deletes any personal data that are not useful or pertinent with the specific Report's investigation and management.

MBE Group ensures that all individuals involved in the Reports have been adequately instructed and bound to confidentiality and that the Reporting Person and Concerned Persons are provided with adequate information pursuant to articles 13 of the GDPR or similar Personal Data protection laws in other regions.

The relationship with external suppliers that process personal data on behalf of MBE Group is ruled by a specific contract pursuant to Article 28 of the GDPR.

Disciplinary Measures

Any breach of this Policy shall be sanctioned in proportion to its severity and in accordance with the applicable laws in force in every country.

Disciplinary actions may be applied also in case of bad faith in the reporting or in any of direct or indirect retaliation applied by any individual within the organization against the Reporting Person.

No disciplinary actions shall be taken against the Reporting Person who files a Report in good faith if the investigation is closed with no evidence of wrongdoing.

5. HOW TO RAISE A REPORT

The Reporting Person shall provide in good faith all information about concerns and/or suspicions regarding any potential or suspected Breach which he/she has become aware of in the Work-Related Context.

The Report should be based on facts and sufficiently detailed with evidence, such as documents, if available. In case of important missing details or information which do not enable an investigation and if MBE Group is not in the position to contact the Reporting Person, due to the anonymity of the Report, the investigation shall not be carried out.

Any fact or information which cannot be disclosed or revealed due to national defense secrecy, medical secrecy, secrecy of judicial deliberations, secrecy of the investigation or the judicial instruction or to the professional secrecy of a lawyer cannot be reported through the Whistleblowing

Channels.

The Reporting Person has the possibility to raise Reports through different Whistleblowing Channels. The Reporting Person may choose the most appropriate channel among the Whistleblowing Channels depending on the specific circumstances of the case.

A. Internal Direct Channel

As a first option, People should normally raise concerns directly with their manager, their representatives from the People Department team, all the members of the management team or any other individuals identified as appropriate reporting contacts (the "**Receiving Person**"), who must treat information received reserved and confidential.

B. Internal Indirect Channel

When the Reporting Person prefers, he or she may choose to file the report through the Internal Direct Channel via contact channels (internet and hotline based) managed by an external provider: NAVEX Global.

Being an independent reporting service, NAVEX Global offers a hotline to Report any Breach – contact channels are available 24/7, through:

- **Website**
  From Web Browser:
  fortidia.ethicspoint.com

- **Mobile / landline call**, using national numbers (TABLE 1 in Annex)

When a Reporting Person contacts the Internal Indirect Channel:

- A customized web form or professional interview specialist will collect the information and document the situation in detail.
- When finished, the Reporting Person will be given a reference number and asked to report back to answer any follow-up questions (in case of anonymous reports the ID associated with the form will be the only way of communicating, no further identity questions will be asked)
- The information is then relayed to our internal process for investigation and follow-up (for details refer to section 6 of this document). All reports are handled promptly and discreetly.
- If the report involves an immediate threat to people or property, NAVEX notifies MBE Group organization immediately so prompt action can be taken.

C. External Channel

Where permitted by Whistleblowing Regulation, the Reporting Person can file the Report to the competent external reporting channels (where existing). The external reporting channels can be mainly used for cases when the Reporting Person:

(a) has already made an internal report that has not been followed-up;
(b) has reasonable grounds to believe that if he/she made an internal report, it would not be effectively followed-up or that the report may lead to risks of retaliation against him or her;

(c) has reasonable grounds to believe that the Breach may present an imminent or obvious danger to the public interest.

6. HOW THE REPORT IS MANAGED

The Reporting Person can choose to raise a report either through the internal direct channel, or by submitting the report through the Internal Indirect channel through Navex.

In case of direct reporting, the Receiving Person is responsible for analyzing the report and evaluating its seriousness. If the report is deemed to be well-founded and serious, the Reporting Person will be invited to open an official Navex Report. If the Person does not wish to open a report personally, the Receiving Person must themselves open an official Navex Report on behalf of the Reporting Person, within maximum 7 days from reception.

Once a report is submitted, receipt will be acknowledged to the Reporting Person within 7 days, including information about support mechanisms.

The Reporting Person will be informed of the measures planned or taken to follow-up the report within 3 months from acknowledgement date. If appropriate follow-up has not been decided within that time, the Reporting Person will also be informed of any further feedback to be expected.

Some concerns may be resolved by agreed action without the need for investigation. If urgent action is required, this will be taken before any investigation is conducted.

If the Navex report is submitted by a Receiving Person on behalf of the Reporting Person, the Receiving Person must manage information exchange throughout the process and shall remain accountable for sharing the final feedback with the Reporting Person once the process has been completed.

Depending on the report, the Chief People Officer who personally leads the investigation will involve or delegate relevant leadership team members, according to their field of competence.

7. REPORTING

The Chief People Officer has overall responsibility for the maintenance and operation of this Policy. The CPO will maintain a record of any Reports raised, always guaranteeing confidentiality as described above, and will report as necessary to the MBE Board.

Documents, information and personal data related to and contained in the Report will be deleted 2 years after the Report is closed.

POLICY NAME	Global Whistleblowing Policy		
EFFECTIVE DATE	VERSION NO.	CONTENT OWNER	DESCRIPTION
15/12/2023	1.0	MBE WW Chief People Officer *Francesca Magrassi*	Policy first release

APPROVALS		
NAME	JOB TITLE	SIGNATURE AND DATE
Flaminia Rezzonico	MBE General Counsel	1/12/2023
Alexandra Williams	USBH General Counsel	5/12/2023
Atalante de Vilallonga	PrestaShop General Counsel	14/12/2023
Kathleen Panek	Chief Corporate Affairs Officer	14/12/2023

ANNEX 1 – NAVEX contacts

Mobile:
mbemobile.ethicspoint.com

Online:
mbeglobal.ethicspoint.com

Call Toll-free:

Country	Telephone
Australia	Dial 1-800-551-155 (Optus) or 1-800-881-011 (Telstra), then dial 844-976-5072
France	Dial 0-800-99-0011 (Orange) or 0805-701-288 (Telecom Development), then dial 844-976-5072
Germany	Dial 0-800-225-5288, then dial 844-976-5072
Italy	Dial 800-172-444, then dial 844-976-5072
Netherlands	Dial 0800-022-9111, then dial 844-976-5072
Poland	Dial 0-0-800-111-1111, then dial 844-976-5072
Spain	Dial 900-99-0011, then dial 844-976-5072
United Kingdom	Dial 0-800-89-0011, then dial 844-976-5072
United States	Dial 844-976-5072

ANNEX 2 – NAVEX ISSUE List

All NAVEX issue standard types are listed in this table:

Issue Name	Issue Description
Accounting and Auditing Matters	The unethical systematic recording and analysis of the business and financial transactions associated with generally accepted accounting practices. (Examples include: misstatement of revenues, misstatement of expenses, misstatement of assets, misapplications of GAAP principles, wrongful transactions.)
Confidentiality and Misappropriation	Confidentiality refers to the protection of the Company's and our customer's non-public information and use of such information only for legitimate business purposes. Misappropriation refers to the unauthorized or improper use of a third party's intellectual property rights, including patents, trademarks, copyrights and trade secrets.
Conflict of Interest	A conflict of interest is defined as a situation in which a person, such as a public official, an employee, or a professional, has a private or personal interest sufficient to appear to influence the objective exercise of his or her official duties. (Examples include: inappropriate vendor relations, bribery, misuse of confidential information, inappropriate customer relations)
Discrimination or Harassment	Uninvited and unwelcome verbal or physical conduct directed at an employee because of his or her sex, religion, ethnicity, or beliefs. (Examples include: bias in hiring, bias in assignments, wrongful termination, bias in promotions, bias in educational decisions, unfair compensation, inappropriate language).
Employee Relations	Any act or omission, which is perceived to be detrimental to the physical or mental well being of an employee.
Gifts and Entertainment	Refers to the inappropriate offering, solicitation or accepting of items of more than nominal value from vendors, customers or other third parties in a capacity as an employee of the Company.
Improper Supplier or Contractor Activity	Supplier or contractor activity in violation of corporate policies and procedures; improper supplier or contractor selection based on personal gain, improper negotiation or diversion of contract awards.
Misuse of Assets or Services	Use of Company resources or equipment without permission for non-business reasons.
Offensive or Inappropriate Communication	The use of inflammatory, derogatory, unduly critical or insulting communication to an employee.
Safety	Failure of meeting requirements needed to perform all duties in a secure environment. Potential areas of harm. (Examples include: environmental damage, OSHA, EPA, supervisor directive, poor housekeeping). Violence is an expression of the intention to inflict evil, injury, or damage to a person or their property. (Examples include: direct, veiled, conditional, violent)

Substance Abuse	Substance abuse is defined as the misuse of both legal and illegal drugs including alcohol. (Examples include: cocaine, narcotics, marijuana, stimulants)
Theft	The act of stealing; specifically: the felonious taking and removing of personal property with intent to deprive the rightful owner of it.
Workplace Violence	A verbal or physical threat of bodily harm to any person currently working or anyone who will be returning to work, allowing the individual who made the threat to carry out the threat.
Other	If you feel that the definitions above do not describe the event, action or situation you are looking to report about, please use this header.