Mustang
Whistleblower Policy

Effective from:	01.07.2022
Version:	1.0

1. Summary

The Mustang whistleblower system is intended to enable employees and other persons to submit anonymous reports. The whistleblower system is intended to record such reports in a comprehensible process that ensures the best possible protection of the legitimate interests of those involved. The purpose of the whistleblower system is to uncover misconduct and prevent both financial damage to the company and a loss of image.

Whistleblowing is intended for the following categories of violations of rules that are relevant or close to criminal law, among others:

- Conflicts of interest,
- corruption and bribery,
- prevention of money laundering and terrorism funding,
- product safety and compliance,
- environmental protection,
- consumer protection,
- protection of privacy and personal data,
- network and information systems security, and
- competition law.

This list contains examples for orientation and does not have any claim to completeness.

This Whistleblower Policy is also intended to ensure, from a technical and organizational perspective, that reports of violations of laws, our Code of Ethics “True Way” or guidelines are received in accordance with the requirements of the Code of Ethics and of data privacy and data security and that they are processed, stored, and archived with the necessary confidentiality.
If local regulations are stricter than the minimum standards laid down in this directive minimum standards, the stricter rules shall apply in each case. If there is a conflict between relevant laws and this Policy, the affected party shall inform the Director Global HR and / or CEO to resolve the conflict.

2. Scope

This policy applies to all executive officers, directors, employees, contracted and temporary workers in all locations worldwide and to all Company representatives, including consultants and agents.

3. Effective date

This policy is effective as of July 1, 2022.

4. Policy contents

4.1. Obligation to report

Any employee and other persons of Mustang are entitled to submit reports. It is irrelevant whether they are employees of Mustang or a subsidiary of Mustang.

To the extent permitted by law and to the extent consistent with conducting an adequate investigation, the company will protect the confidentiality and anonymity of the person making the report.

This policy does not imply any requirement for anyone to report. However, if there are legal, contractual, or other duties or obligations to provide reports, these are not affected by the above paragraph.

4.2. No act of retaliation

Employees and others who report will not be harassed, retaliated against, or suffer adverse employment consequences, such as discharge, demotion, suspension, discrimination with respect to the terms and conditions of employment.

Employees and associated persons who retaliate against an individual who has reported an incident in good faith will be subject to disciplinary action, up to and including termination.

4.3. Submission of reports

The submission of reports of actual or suspected violations shall be made possible as described below:

- Reports can be reported confidentially to the direct supervisor; the head of department, the human resources department or the works council
- Reports can be reported directly and confidentially to the compliance department;
- Reports can be reported directly and confidentially via the digital whistleblower system.

In the digital whistleblower system, the forms of reports are technically predefined. In all other cases, however, the submission of reports is not bound to specific forms. An up-to-date overview of the reporting channels can be found in the current version of our Code of Ethics.

4.4. Relevant reports

The whistleblower system is provided solely for the purpose of receiving and processing reports of any alleged or actual violations of laws, policies, or the Code of Ethics. It is not available for general complaints or for product and warranty inquiries.

Only those reports should be submitted where the whistleblower believes in good faith that the information provided by him/her is correct. The person is not in good faith if he/she knows that a reported fact is untrue. In case of doubt, corresponding facts are not to be presented as a fact, but as an assumption, evaluation or as a statement of other persons.

It is noted that a whistleblower may be liable to prosecution if, against his or her better knowledge, he or she alleges untrue facts about other persons.

4.5. Protection of the whistleblower

All reports, including references to the whistleblower, will be processed confidentially and in accordance with applicable laws.

4.6. Legal restrictions

The laws in some countries prescribe certain restrictions for reports, e.g., what may be reported, whether personal data about an individual may be stored, or whether reports can be made anonymously. The corresponding requirements are integrated into the digital whistleblower system. Any concerns that cannot be reported using the mentioned reporting procedures due to such restrictions should be directed to the employee's supervisor. If an employee feels that it is not possible to raise the matter locally, they should escalate it within the business unit to the local HR representative.

5. Confidentiality and data protection

All reports, regardless of their truthfulness, are likely to damage the reputation of the persons concerned, the whistleblowers and / or third parties as well as the company fully.
We therefore treat them with confidentiality, over and above the obligations arising from the data protection laws.

In addition to the register of data processors, which must be always kept up to date, a written record must be kept of the persons who may work with related data and what rights they have in the context of data processing. These persons must be obligated to observe special confidentiality over and above any legal requirements.

6. IT and data security

IT solutions for the intake and processing of reports must be approved by the Data Protection Officer before they are used.

The minimum requirements for the scope of the General Data Protection Regulation are derived from Art. 32 of the GDPR, the Group guidelines on IT security and data protection.

The sensitivity of the information and the risks to persons and the company if data relating to the information becomes known must be considered in a special way.

7. Deletion of data

The deletion of data in the digital whistleblower system must be carried out exclusively in accordance with the respective time specifications of the deletion concept or after deletion approval by two separate users (four eyes principle).