# SMC Morocco WHISTLEBLOWER POLICY

## Purpose of the Policy:

The Whistleblower Protection Policy document defines the main lines of SMC's policy and the procedure to be followed by staff members, including persons whose employment relationship ended when the information was obtained. within the framework of this relationship, the persons who applied for a job within SMC when the information was obtained within the framework of this application, the temporary employees and the temporary or seconded personnel within SMC, the shareholders, partners, members of administrative and management bodies, co-contractors and sub-contractors in the event of irregularities, non-compliance or presumed reprehensible behavior as specified below.

It provides for the protection measures granted to interested parties who in good faith report such facts. Given the importance of guaranteeing data security and confidentiality to employees, SMC has decided to supplement its existing internal whistleblowing process with a digital internal whistleblowing system managed by a certified company, EQS Group, which guarantees high security standards, in particular thanks to a secure end-to-end data encryption system and computer protection and security mechanisms that meet the most demanding standards.

SMC's whistleblowing policy falls within the framework of the ethical and business principles enshrined in the Group Code of Conduct and is intended to preserve the interests of SMC and its employees by facilitating prevention. and the detection of possible irregularities or abusive practices.

## Definitions:

Reports may relate in particular to:

- Acts of corruption, conflicts of interest, tax evasion, breach of trust...
- Facts contravening the safety of the premises or the safety and conformity of the products (rules of health and safety, environment, waste management, etc.)
- Facts constituting violations of human rights or fundamental freedoms, the health or safety of persons
- Facts likely to infringe the rules of competition and economic regulation

- Facts about data protection and IT security
- Acts of moral or sexual harassment
- Facts contrary to the Group's code of conduct or likely to harm its interests

and harm it

Information covered by defense secrecy, medical secrecy, secrecy between a lawyer and his client as well as the secrecy of judicial deliberations, investigation and instruction are excluded from the system of the right to alert.

The whistleblower is protected by law, as are all people called "facilitators" (unions, associations, colleagues, relatives) who have helped the whistleblower to report information relating to the facts denounced.

### What is the purpose and scope of the alert system?

The right to alert recognized by the aforementioned laws is not an obligation but an option offered to any employee to decide in full conscience whether or not to report or reveal a serious breach of the general interest or the regulations of which he is aware.

The purpose of the alert is to remedy or put an end to serious malfunctions, violations of laws, rights and freedoms or attacks on the general interest noted by the employee. The alert does not relate to an individual or collective labor dispute.

The alert must be able to be processed in time by the company. However, it may be immediately made public if the seriousness and urgency of the alert justify it.

## Reporting procedure:

### How to submit a report?

- Internal reporting: Collection procedure

Generally, reports may be written, including via internal messaging, or oral (by telephone and at the request of the reporting person through a face-to-face interview within a reasonable timeframe) or both.

To strengthen its internal alert system and guarantee whistleblowers the protection and confidentiality of their data and the optimal follow-up of reports, SMC has set up a secure alert system accessible to all and strictly respecting the regulations.

The whistleblower can now send his report to SMC via the service provider EQS Group AG (“EQS”) at the address https://smc.integrityline.com/

When the whistleblower submits a report, he has the option of creating a secure, anonymous mailbox if he wishes (without leaving an email address), giving rise to a file reference and a password system. secure password, allowing him to exchange in complete confidentiality directly with the referent in charge of processing the file. In this case, it is advisable to consult the mailbox regularly in case additional information is necessary.

An acknowledgment of receipt of the report will be issued within 8 days.

- External reporting: Defender of Rights, administrative or judicial authorities, professional order, etc.

In the event that the whistleblower opts for this external reporting mode directly or after entering the internal reporting channel, he must refer to the reporting methods indicated by the recipients of the external reporting.

### Information to be provided in the event of a report:

The alert must be established in good faith on the basis of precise factual elements and not erroneous or misleading information. People who report reprehensible behavior must provide all useful information, in particular by producing written documents (letters, reports, documents, etc.) or other evidence.

The whistleblower must avoid any generalization, any exaggeration or any accusation not supported by proof, in order to stick to the facts necessary to process the alert and not expose themselves to prosecution for slanderous denunciation.

Under these conditions, he will be protected by benefiting from the legal status of “whistleblower”. »

## Privacy :

Reporters are assured of the confidentiality attached to the internal reporting system set up by SMC, in particular through the use of the secure alert platform EQS Integrity and its mailbox system facilitating exchanges and guaranteeing the confidentiality of information transmitted.

Items likely to identify the whistleblower may only be disclosed with the latter's consent. They may, however, be communicated to the judicial authority, in the event that the persons responsible for

collecting or processing the reports are required to report the facts to the latter. The whistleblower is then informed, unless this information risks compromising the legal proceedings.

The elements of the report file will be used exclusively for the purposes of processing the report and will be destroyed within a maximum of two months from the closing of the file.

If desired, the whistleblower can choose to report anonymously and request anonymity throughout the case follow-up process.

In all cases, the EQS system allows processing of the alert report in encrypted form and all communications are made via a secure connection.

## Protection of personal data :

In the event of a non-anonymous report, personal data may be used for administrative purposes, in particular the management of the report register and the alert line implemented with the company EQS, a company with which SMC has concluded an agreement. processing of personal data in accordance with the Privacy Policy of SMC.

SMC and EQS undertake to respect the Privacy Policy for personal data that may be transmitted as part of the reporting process, in particular by adopting appropriate technical and organizational measures and by processing the data under conditions that comply with the legal framework throughout. throughout the whistleblowing investigation procedure, while respecting the rights of the persons concerned.

## Investigation of suspected cases of misconduct:

Upon receipt of the alert, the author of the report receives an acknowledgment of receipt and possibly requests for clarification. Secure exchanges are possible throughout the file processing process via the secure mailbox hosted by the EQS platform.

The decision to undertake a control, an audit or any other type of investigation is taken on a case-by-case basis by the Chairman and CEO of SMC France, who is also the statutory head of SMC Morocco, after examining the serious nature of the facts invoked and the accuracy of the information given. The decision is taken as quickly as possible according to the specifics of the file, at the latest within 90 days of receipt of the report (no more than 3 months).

The author of the report is informed within the same deadlines of the follow-up measures that may be taken following his report.

## Whistleblower protection system:

The disclosure of the identity of the whistleblower without his consent, except to the judicial authority, is criminally sanctioned.

The whistleblower may not be held liable either civilly for the harm that his report in good faith will have caused, nor criminally for having intercepted and taken away confidential documents related to his alert, containing information to which he will have had lawful access. .

Criminal penalties, up to three years in prison and heavy fines, are provided for by law in the event of retaliation or infringement of the rights of whistleblowers. The texts also provide for the impossibility of resorting to any method likely to destabilize the employee: disciplinary sanction, demotion, refusal of promotion, disadvantageous treatment, placing on a "blacklist", intimidation, damage to reputation, etc.

In the event that the whistleblower disputes a possible reprisal measure, he may benefit from a provision for legal costs from the judge.

In the event of legal proceedings against whistleblowers, their authors will have the obligation to advance the legal costs.