www.smt.network

WHISTLEBLOWING POLICY

SMT

25 March 2025

DOCUMENT INFORMATION

Author(s)	:	Legal & compliance department
Subject	:	Whistleblowing Policy
Version	:	1
Date	:	25 March 2025

Revision	Date	Author(s)	Adjustment description	Check	Appr.

Table of contents

Page

1 Purpose 4

2 Scope 4

3 Ownership 4

4 Definitions 5

5 Reporting process 5

5.1 Which types of conduct should be reported? 5

5.2 How to make a report? 6

5.3 Identity protection guaranteed 6

5.4 Retaliation protection guaranteed 7

5.5 How do we assess a report? 8

1 Purpose

The purpose of this policy is to provide a clear set of guidelines on the approach and management of the reporting of (suspected) illegal acts, unethical behaviour, misconduct or other serious concerns, by any internal or external stakeholder who has whistleblowing rights in accordance with the applicable whistleblowing regulations.

All stakeholders need to know that they can provide information on any serious concern they have, understand where they can report their concerns, know what happens after they make a report, and ensure they feel safe in filing a report.

Everyone should be able to make a report anonymously. We are committed to protect the identity of the whistleblowers and they only need to reveal their identity if they choose to do so.

We are committed to protect whistleblowers who make reports in good faith against retaliation measures.

2 Scope

The whistleblowing policy applies to all internal and external stakeholders who have whistleblowing rights in accordance with the applicable whistleblowing regulations. Are considered as internal stakeholders: employees (including expats), directors and shareholders. Are considered as external stakeholders: former employees, applicants, freelancers, contractors and suppliers. The rights and protections laid in this policy cannot be waived by any agreement, policy, form or condition of employment.

If any jurisdiction where we operate has whistleblowing protection laws that provide a higher level of protection than what is included in this policy, the local legislation shall take precedence.

3 Ownership

The whistleblowing policy is managed by the whistleblowing committee. Changes to the whistleblowing policy require prior approval from the whistleblowing committee.

4 Definitions

Whistleblowing Committee
The committee consists of Head of Compliance Group, Head of Legal Group and Chief Digital & Information Officer SMT Holding SA/NV.

Independent Whistleblowing Officer (IWO)
The whistleblowing committee has designated Lighthouse Compliance Consultants as the Independent Whistleblower Officer (« **IWO** ») who will act as the sole recipient of the whistleblowing reports. This guarantees the confidentiality of the whistleblower.

Whistleblowing system
An encrypted third-party system compliant with ISO 27000 which we use to enable stakeholder reporting, both nominative and anonymously, on any type of illegal acts, unethical behavior, misconduct or other serious concerns. The whistleblowing management system is available at https://SMT.safewhistleblowing.solutions

5 Reporting process

5.1 Which types of conduct should be reported?

There is no intention to limit the topics of serious concerns to be reported: in principle any form of serious concern can be reported, provided that this is done in good faith. Hence, the following types of (suspected) illegal acts, unethical behaviour, misconduct and other serious concerns are to be reported immediately:

- Fraud & Misappropriation of assets;
- Bribery & Corruption;
- Collusion & Conflicts of interest;
- Blackmail;
- Non-compliance with antitrust or competition laws;
- Data theft & Data leakage;
- Corporate espionage;
- Violations of accounting rules/shareholder rights;
- Environment, Health & Safety issues;

- Unethical behaviour, including harassment or bullying of any kind;
- Non-compliance with internal regulations; and
- Other serious concerns.

The whistleblowing system is not to be used for reporting of day-to-day concerns to the extent they cannot be qualified as illegal acts, unethical behaviour, misconduct or other serious concerns. The whistleblowing system should not be used by employees for raising routine grievances about their personal employment situation.

Serious concerns may be reported even without supporting evidence; reasonable suspicions that wrongdoing took place, is taking place or is about to take place is sufficient.

If you have raised a serious concern in good faith, the process and all those involved in its implementation will support and protect the whistleblower. However, if a false concern is raised in bad faith (e.g., for malicious reasons or on the basis of false statements), the whistleblower may be subject to disciplinary action, in accordance with the applicable rules and policies, up to and including termination of employment, as well as referral to judicial authorities.

5.2 How to report?

If a stakeholder would like to make a report, he or she should use the secure whistleblowing system which allows the written reporting on a named or anonymous basis, accessible on this platform: https://SMT.safewhistleblowing.solutions. You can there find more details on the reporting process.

Whistleblowers based in the EU also have the right to report directly to the competent authorities assigned by the EU Member State where the reporting takes place. In the event the whistleblower uses the right to report to competent authorities he or she is advised to do so by use of encrypted mail sent by private WIFI, to avoid data interception by or leakage to third parties. We recommend that the stakeholder first makes a report internally by use of the secure whistleblowing system.

5.3 Identity protection guaranteed

The IWO will act as identity protection manager. The IWO will not reveal the identity without the prior approval of the whistleblower. Before this approval has been obtained, the content of the report can only be shared with the whistleblowing committee.

The IWO will organize the access to the case details for all other internal functions and external parties. In order to guarantee a confidential reporting setup, an access to case details for other internal functions and external parties can only be granted upon prior request of the whistleblowing committee and prior approval of the whistleblower.

The whistleblower can remain anonymous throughout the assessment of the report. At any given time, the whistleblower can identify him/herself, however at no point he or she will be forced to provide her/his identity. It is worth noting that we will make every possible endeavour to investigate all admissible reports, but in some cases, there are limitations to what can be achieved if the whistleblower decides to remain anonymous. If the whistleblower decides to disclose his/her identity, matters raised will be treated in strictest confidence and will be investigated discreetly.

5.4 Retaliation protection guaranteed

We will take the necessary measures to prohibit any form of retaliation against whistleblowers (including threats and attempts of retaliation) particularly – but not limited to - in the form of:

- suspension, demotion or withholding of promotion and withholding of training;
- negative performance assessment or employment reference;
- any disciplinary measure, reprimand or other penalty;
- coercion, intimidation, harassment, discrimination or unfair treatment;
- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
- failure to renew, or early termination of, a temporary employment contract;
- harm, including to the person's reputation (particularly in social media) or financial loss, including loss of business and loss of income;
- blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may cause that the person will not find employment in the sector or industry; or
- early termination or cancellation of a contract for goods or services.

We ensure that support measures are put in place for whistleblowers, where appropriate. We will draw appropriate consequences, as per our internal procedures, against any natural or legal persons that:

- hinder or attempt to hinder reporting;
- retaliate against whistleblowers;
- bring vexatious proceedings against whistleblowers; and
- breach the duty of maintaining the confidentiality of the identity of whistleblowers.

The whistleblower should be able to make reports on illegal acts, misconduct and other serious concerns without any fear of retaliation. A whistleblower is protected against any negative decision

which is linked to the act of whistleblowing. If the disclosing of the whistleblower's identity is followed by a negative decision, he or she shall have the right to request the whistleblowing committee to prove that there is no link between the report and the negative decision (reversed burden of proof).

We speak of a "*serious risk of retaliation*", when the whistleblower believes retaliation is near or imminent. In such event, the whistleblower should contact the IWO, who will then inform the whistleblowing committee. The whistleblowing committee will decide on steps to protect the whistleblower from a serious risk of retaliation of which the whistleblower will be informed. Although whistleblowers are invited to share their insights on possible useful steps to avoid retaliation, the whistleblowing committee is not obliged to follow them.

Other parties that might have to bear witness or are involved in the investigation will be protected from retaliation (insofar the conditions are met) in the same manner as the whistleblower.

5.5 How do we assess a report?

Hereunder, find the different steps that will be initiated once a report is received:

- Report (nominative or anonymous) is received;
- The IWO as sole recipient of all the reports will notify the receipt of the report within maximum 7 days;
- The IWO will perform an initial assessment of the report and interact with the whistleblower if more details or clarifications are needed;
- The whistleblowing committee will receive the assessment of the IWO;
- Based on the recommendations made by the IWO, the whistleblowing committee will decide on risk classifications and follow up measures;
- The whistleblower will be informed about either the case rejection or the case acceptance within 1 month of the report; and
- After the notification of the case acceptance, the case will be scheduled for status reporting. In this case, the whistleblower will receive a status report within maximum 3 months of the report with an overview of the follow up measures and results.

If, after receiving the case rejection decision or status report, the whistleblower is not satisfied, he or she can escalate this to the IWO, who will then inform the whistleblowing committee. Based on the recommendations made by the IWO, the whistleblowing committee will decide on any follow up measure of which the whistleblower will be informed. Although whistleblowers are invited to

share their insights on possible useful follow up measures, the Whistleblowing Committee is not obliged to follow them.

SMT

SERVICES MACHINERY TRUCKS

www.smt.network