INTERNATIONAL SOS

Whistleblower Policy

Linked to:

International SOS Code of Conduct and Ethics
Fraud and Corruption Control Policy

Version 2.01

POLICY

Document Owner: **Legal**

Document Manager: **Chief Security Officer**

Effective: **June 2015**

Updated: ***March 2024***

WORLDWIDE REACH.
HUMAN TOUCH.

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Purpose

1.1.1. The Whistleblower Policy is one of a number of Policies and Codes that promotes a culture of integrity, honesty and ethical behaviour within the International SOS Group.

1.1.2. International SOS's aim is to encourage staff to report any suspected breach of our Code of Conduct and Ethics, professional standards or law (wrong-doing) in good faith and in an environment free from victimisation so that senior management can adequately identify issues and manage risk within the group.

1.1.3. The Whistleblower Policy does not prevent a staff member from reporting suspected wrongdoing to a regulator under an applicable law or prudential standard.

1.2. Objectives

1.2.1. State the International SOS policy for reporting of suspected wrongdoing.

1.2.2. Describe avenues for reporting of suspected wrongdoing.

1.2.3. Define protection arrangements for individuals who report suspected wrongdoing (Whistleblowers).

1.3. Scope

1.3.1. The Whistleblower Policy applies to all employees, contractors, consultants and clients in all businesses and subsidiaries within the International SOS Group.

1.3.2. It sets out the minimum requirements for the International SOS Group. Business units that operate in jurisdictions that legislate a higher standard are to follow those local regulations and adopt appropriate local procedures.

1.4. Definitions

1.4.1. **Whistleblower.** An employee (full or part time), intern, contractor, consultant or client who exposes suspected misconduct, dishonest or illegal activity occurring in International SOS.

1.4.2. **Wrongdoing.** Examples of Wrongdoing include, but are not limited to, the following:

a) a breach of the International SOS Code of Conduct and Ethics;

b) a breach of regulations or laws;

c) a breach of International SOS's Policies and Procedures;

d) dishonest or corrupt behaviour, including soliciting, accepting or offering a bribe, facilitation payments or other such benefits;

e) bullying, harassment (sexual or otherwise) or discrimination;

f) fraudulent activity;

g) illegal activity (including theft, drug sale / use, violence or threatened violence and property damage);

h) impeding internal or external audit processes;

i) improper behaviour relating to accounting, finance, or audit matters;

j) conduct endangering health or safety;

k) breaches of professional standards (such as medical standards);

l) mismanagement of the Group's resources;

m) conduct that is detrimental to International SOS's financial position or reputation; and

n) concealment of Wrongdoing.

2. REPORTING WRONGDOING

2.1. Reporting Channels

2.1.1. Suspected Wrongdoing may be reported via the following channels:

a) Via their management chain

b) Via the Hydra – Incidents system or MS Word (paper) report

c) Direct to their HR Director, the Group Manager Compliance, or the Chairman and Chief Executive Officer.

d) By using the hotline and incident management systems, as detailed in paragraph 2.5 below.

2.2. Management Chain

2.2.1. Employees are encouraged to first discuss their concern with their immediate managers unless they suspect involvement or compromise of these personnel.

2.2.2. Any employee who receives a report of suspected Wrongdoing must treat the matter confidentially and in accordance with this policy. An employee who submits a report of suspected Wrongdoing should use discretion in discussing the topic with others (outside this policy) as this may negatively impact the Company's ability to address the matter appropriately.

2.2.3. Immediate managers who receive reports of alleged Wrongdoing must escalate these cases to ensure appropriate consideration of the report. Escalation may be made to their relevant HR Director, the Country General Manager or the Group Manager Compliance using one of the reporting channels listed above.

2.2.4. If employees do not feel comfortable speaking with their immediate manager, they can report their concern via one of the alternate reporting mechanisms described below.

2.3. Hydra-Incidents System

2.3.1. Hydra is the name of the application used for customer feedback, incident reporting and management, risk management and quality management within International SOS. Hydra – Incidents supports adverse incident reporting and incorporates automatic escalation to line management and functional management.

2.3.2. There are two mechanisms for recording the details of an incident in Hydra:

a) Completion of a report via the ROAM application – allows one-way reporting of key sections of the incident report, or

b) Direct entry of the incident into Hydra by an *Authorised User*. All incidents are entered into Hydra with the exception of Clinical Incidents which are managed in the local Clinical Incident Register.

2.4. Nominated Managers

2.4.1. Reports can be made via email to an employee's regional HR Director or to the Group Manager Compliance at Compliance@internationalsos.com.

2.5. Anonymous Reporting – Hotline and Incident Management Systems

2.5.1. International SOS' electronic reporting platforms enable staff, customers or service providers to anonymously report any suspected breach of our Code of Conduct and Ethics, professional standards or applicable laws. Both systems are accessible via Insite as well as on the Compliance page of Insite:

2.5.1.1. Reporting involving a situation within the International SOS Group, except for contracts supporting the Government Services Division, should be reported through the "Integrity Reports" link: https://intlsos.portal.speeki.com.

2.5.1.2. Reports involving International SOS Government Services Division should be sent through the "EthicsPoint" link: https://secure.ethicspoint.com/domain/media/en/gui/59418/index.html

2.5.2. The applications allow seamless communication between an anonymous reporter and the designated corporate officer. Initial reports are accessible only to the designated offices. In the case of non-government services: Chief Security Officer and Group Senior Manager Compliance, in the case of Government Services: Government Services Division VP of Contracts & Compliance as well as the Government Services Regulatory Compliance Specialist. In both cases these teams will escalate reports to the Group General Counsel.

2.5.3. Contact with any Whistleblower is governed by strict procedures that are designed to protect the identity of the individual. Staff involved in the communications and subsequent investigation must not attempt to identify the Whistleblower and, unless the Whistleblower otherwise consents and subject to applicable law, must protect the Whistleblower's identity in the event it becomes known.

2.6. Local Reporting Channels

2.6.1. Where required by local regulations, the Country General Manager shall adopt and raise awareness on appropriate local internal and external reporting channels which may differ to the ones listed in paragraphs 2.1. to 2.5. above.

3. REPORT FOLLOW UP

3.1. Management Responsibilities

3.1.1. Reports of suspected Wrongdoing raised through these channels must be escalated to the relevant country or functional general manager or divisional head, unless they are implicated in the alleged wrongdoing.

3.1.2. All incidents are to be investigated in accordance with the International SOS Investigation Procedures, which require a preliminary investigation (to ascertain whether there are sufficient grounds to launch an investigation), establishment and sign off of terms of reference, approval by the Group General Counsel and conduct of a formal investigation. The Intl.SOS Investigation Procedures is available on InSite under: Reference Point / Procedures / Investigation Procedures.

3.1.3. The extent to which a report can be investigated will be limited by the details contained in the report submitted by the Whistleblower. For a report to be investigated, it must contain sufficient information to form a reasonable basis for investigation.

3.1.4. The extent of the investigative effort will be shaped by the severity of the alleged wrongdoing.

3.1.5. A Whistleblower must be protected and reassured that the investigation will be conducted in accordance with the principles of fairness and confidentiality.

3.2. Whistleblower Responsibilities

3.2.1. Reporters are entitled to protection under this Policy if they have reasonable grounds to believe, in light of the circumstances and the information available to them at the time of reporting, that the maters reported by them are true. Employees must report incidents honestly. Reports that are found to be intentionally dishonest will be investigated under our Code of Conduct and Ethics.

3.2.2. Employees reporting anonymously should provide as much information as possible so as not to compromise the ability to fully investigate the report.

3.2.3. A Whistleblower will always have access to a report submitted on the “Integrity Reports” application and will be informed of the outcome of the investigation, via the reporting application. In cases where the investigator has not substantiated the allegations, an appropriate explanation will be made to the Whistleblower, subject to any privacy and confidentiality rights.

3.3. Whistleblower Protection Officer (WPO)

3.3.1. The Group Manager Compliance serves as the Group Whistleblower Protection Officer (WPO). The WPO is responsible for protecting the Whistleblower from being victimised as a result of making a report.

3.3.2. Any staff member reporting suspected Wrongdoing can seek advice from the WPO prior to or after making a report.

3.3.3. The WPO can protect the Whistleblower in a number of ways including, but not limited to, the following:

a) Ensuring confidentiality in the investigation.

b) Protecting, as far as legally possible, the staff member's identity.

c) Coordinating a leave of absence while a matter is investigated.

d) Coordinating the relocation of the Whistleblower or other staff to a different work group or department.

3.4. Reporting and Governance

3.4.1. The Group Senior Manager Compliance reviews the reports submitted through Hydra – Incidents and "Integrity Reports" and all escalated issues.

3.4.2. The Government Services Division VP of Contracts & Compliance or the Regulatory Compliance Specialist reviews the reports submitted via EthicsPoint and all escalated issues related to Government Services Division contracts.

3.4.3. A consolidated report is to be developed by the Group Manager Compliance and reviewed on an annual basis by the AEA Board.

3.4.4. The Policy is reviewed in accordance with the International SOS Documents Policy and whenever there are significant regulatory changes or new business needs. The Intl.SOS Documents Policy is available on InSite under: Reference Point/Group Policy.

3.4.5. Reports are to be retained in adherence to the International SOS Data Retention, Archiving and Destruction Policy.

3.5. Data Protection

3.5.1. Reports and any notes recorded in the Integrity Reporting system will be retained for a maximum period of 12 months after the conclusion of any investigation.

3.5.2. Reports and any notes recorded in the EthicsPoint system will be retained according to standards imposed by the Federal Acquisition Regulations as specified in the US Government contract requirements or any other regulatory requirements based on the contract requirements.

3.5.3. At the end of this period the entries will be automatically deleted.

4. ENFORCEMENT AND REPORTING BREACHES

4.1. Breaches of this Policy may have serious legal and reputation repercussions and could cause material damage to International SOS. Consequently, breaches can potentially lead to disciplinary action that could include summary dismissal and to legal sanctions, including criminal penalties.

4.2. All employees are expected to promptly and fully report any breaches of the Policy. A report may be made to the employees' supervisor or the Group General Counsel. Reports made in good faith by someone who has not breached this Policy will not reflect badly on that person or their career at Intl.SOS. Reports may be made using the following e-mail address: Compliance@internationalsos.com.