

---

# **Whistleblower Policy IATS Management System**

Document No.: D6990-081

Version: 01.00.00

---

# Contents

- 1. INTRODUCTION .....3**
  - 1.1 Purpose..... 3
  - 1.2 Scope..... 3
  - 1.3 Responsibility..... 3
  
- 2. WHISTLEBLOWER POLICY .....4**
  - 2.1 Background and purpose .....4
  - 2.2 Who can be reported? .....4
  - 2.3 What matters can be reported? .....4
  - 2.4 How is a report made?.....5
  - 2.5 Who receives reports? .....5
  - 2.6 Procedures for receiving a report .....5
  - 2.7 Investigation of a report .....5
  - 2.8 Duty of confidentiality and disclosure of information .....5
  - 2.9 Anonymity, protection against retaliation and other whistleblower rights .....6
  - 2.10 Ongoing communication and deadlines .....6
  - 2.11 Confidentiality .....6
  - 2.12 Registration of reports .....6
  - 2.13 Rights of persons concerned.....7
  - 2.14 External whistleblower scheme .....7
  - 2.15 The whistleblower´s right of publication .....7

# Tables

- Table 1: Version History .....2

# Version History

Version	Date	Prep.	App.	Change Description
01.00.00	2024-12-12	MITA	ERBO	First release

**Table 1: Version History**

# **1. Introduction**

## **1.1 Purpose**

This document describes the Insero Air Traffic Solutions (IATS) Whistle Blower Policy and forms part of the IATS Management System.

## **1.2 Scope**

This document applies to all of IATS.

## **1.3 Responsibility**

This document is maintained by the IATS Quality Manager and shall be approved by the IATS Chairman of the Board.

## 2. Whistleblower Policy

### 2.1 Background and purpose

Insero Air Traffic Solutions (IATS) is making a whistleblower scheme, primarily for our employees but it may also be used by external 3<sup>rd</sup> parties.

A whistleblower scheme is an independent channel where employees can report suspicions or specific information about serious violations or other serious matters in IATS.

The whistleblower scheme should be seen as a supplement to the opportunity you have as an employee to go to someone in management if you find faults or unsatisfactory matters you want to draw attention to.

This whistleblower policy describes in more detail when you can use the whistleblower scheme, what you can report, how a report is handled, rights for those involved, etc. In addition to this information, IATS has drawn up a privacy policy which specifically concerns the processing of personal data in connection with the whistleblower scheme. It forms part of the IATS Management System and is titled, D6990-082, IATS Whistleblower Privacy Policy.

The whistleblower scheme applies to all employees of IATS. It also applies to persons with fixed-term employment or temporary staff as well as external 3<sup>rd</sup> parties.

### 2.2 Who can be reported?

The whistleblower scheme should be used to report information and matters relating to violations and serious failings by employees or other persons associated with IATS.

### 2.3 What matters can be reported?

Both violations of EU law, serious violations of Danish law and other serious matters can be reported, as long as the matters concern persons connected with IATS, cf. above.

A report may relate to a suspicion or actual knowledge of violations in, for example, the following areas:

- Public procurement/tendering
- Money laundering and terrorist financing
- Protection of privacy and security of network and information systems
- Consumer protection
- Economic crime, such as embezzlement, theft, bribery, fraud and forgery
- Hacking, tapping, recording conversations between others, etc.
- Violations of legislation on accounting, tax, etc.
- Violations of confidentiality
- Neglect of statutory duty to act
- Violation of rules on the use of force
- Serious and repeated violations of legal principles
- Deliberate deception of citizens and partners
- Physical and psychological violence and sexual abuse or serious harassment based on e.g. race, gender, language, wealth, national or social origin, political or religious affiliation
- Neglect of professional standards that might pose a risk to e.g. the safety and health of persons
- Failure of care
- Serious or repeated violations of the workplace's internal guidelines on e.g. business trips, gifts and financial reporting
- Serious faults and serious irregularities associated with IT operation or IT system management.

The above is a non-exhaustive list of examples.

The whistleblower scheme does not apply to information of a trivial nature or information on e.g. violation of internal guidelines on sick leave, smoking, alcohol, clothing, private use of office supplies, or violation of ancillary rules, such as non-compliance with documentation requirements.

However, in the case of systematic violations, it may well be that these otherwise less serious matters may be covered by the whistleblower scheme. The whistleblower scheme cannot be used to report on your own employment relationship, including conflicts between employees, cooperation issues or matters that come under the system of

trade union law (serious harassment and sexual harassment are, however, covered, cf. the above, and cooperation issues are covered if they are deemed to be sufficiently serious to pose a genuine risk to human life and health).

Information on violations or matters that have taken place prior to IATS's establishment of a whistleblower scheme may be reported.

## 2.4 How is a report made?

IATS's employees and external stakeholders can report anonymously in writing.

You will find a link to the whistleblower scheme and reporting solution here: <https://ineroats.com/Whistleblower>.

## 2.5 Who receives reports?

Information in a report is received by the IATS Chairman of the Board (hereinafter the "Recipient"), who handles reports received via IATS's whistleblower scheme. When the Recipient has received a report:

- the Recipient screens the report, including for which level at the company the report concerns,
- the Recipient confirms receipt of the report to the whistleblower,
- The Recipient handles the issue.

We have chosen this particular solution because we want to create the greatest possible sense of security for IATS's employees in connection with a report.

## 2.6 Procedures for receiving a report

When a report is received, an assessment is made of whether the report falls within the scope of the whistleblower scheme, cf. section 3.

If the report falls outside the scope of the whistleblower scheme, it will be rejected and cannot therefore be handled within the framework of the whistleblower scheme.

If a report falls outside the scope of the whistleblower scheme, the whistleblower will receive guidance on where they can instead raise the matter in question within IATS.

## 2.7 Investigation of a report

Once the Recipient has received the report, Recipient must carry out a thorough follow-up which, depending on the circumstances surrounding the report, may include:

- Initiating an internal investigation to confirm or refute the accuracy of the information in a report
- Briefing IATS's board of directors
- Reporting to the police or relevant supervisory authority
- Deciding on responses, e.g. under employment or contract law
- Closing the case

Recipient is responsible for requesting that the report be thoroughly investigated and taking the necessary measures in this regard.

Subsequently, Recipient must prepare a statement for the IATS board of directors, which will then decide on the response, whether reporting to the authorities or other responses under employment or contract law.

Finally, feedback must be given to the whistleblower within the 3-month deadline stipulated in the whistleblower scheme, cf. section 10 below.

## 2.8 Duty of confidentiality and disclosure of information

Only the Recipient has access to the information in a report. Reports are subject to a special duty of confidentiality, and the content may therefore not be disclosed to others.

The special duty of confidentiality only applies to information in a report, and if further information emerges as part of a further investigation, such information is not covered by the special duty of confidentiality. For this information, the general rules on disclosure and access to documents apply.

If the whistleblower has waived their anonymity, the special duty of confidentiality no longer applies to the information included in the report. Similarly, IATS is entitled to share information from a report, including the identity of the whistleblower, if this is known, with e.g. the police. In such cases, the whistleblower must be informed.

## 2.9 Anonymity, protection against retaliation and other whistleblower rights

As a whistleblower, you have the right to remain anonymous throughout the process. The contact details for the whistleblower is solely available to the Recipient and provides the opportunity to communicate anonymously with the Recipient of the reports, without this information becoming available to IATS.

However, a report may be of such a nature that it can be difficult to thoroughly investigate a matter without the whistleblower choosing to come forward and thus waive their right to anonymity. It is the whistleblower's own decision whether this should happen. If anonymity is waived, the intention of the Whistleblower Directive is to protect the whistleblower from, among other things, any form of retaliation or threat, or attempts at retaliation, that occur as a result of the whistleblower making a report. Retaliation is to be understood as any kind of adverse treatment or adverse consequence that occurs as a reaction to a report. This might e.g. be suspension, dismissal, demotion or lack of promotion, transfer of duties, transfer, pay cut, disciplinary action, coercion, intimidation, harassment, discrimination, etc.

Being mentioned in a report can have significant consequences, and the whistleblower is therefore required to act in good faith regarding the content of a report. A deliberately false report from a whistleblower, e.g. relating to harassment, may lead to criminal consequences for the whistleblower.

On the other hand, a whistleblower cannot be held liable for disclosing confidential information if the whistleblower had reasonable grounds to believe that the information disclosed in the form of a report was correct at the time the report was made and that the information concerned serious violations or other serious matters covered by the scheme.

On this basis, the whistleblower will also not be held responsible for having gained access to the information that has been reported. However, this presupposes that the act by which access was gained does not in itself constitute a criminal act – e.g. burglary.

## 2.10 Ongoing communication and deadlines

The recipient handles the communication with the whistleblower via the whistleblower system.

A whistleblower must receive confirmation of receipt of a report no later than 7 days after submitting their report.

In addition, the whistleblower must receive feedback as soon as possible, and no later than 3 months from confirmation of receipt, which means that – to the extent possible – the whistleblower must be informed of what measures have been taken, or are intended to be taken, and why this specific type of follow-up has been chosen. In connection with feedback, some information cannot be shared with the whistleblower, e.g. due to a statutory duty of confidentiality, personal data legislation, etc.

In addition to information about the chosen follow-up, the whistleblower must, to the extent possible, also be given information about the course of the investigation and the outcome, if this can be done within the applicable rules.

If, due to the circumstances of the case, it is not possible to give final feedback before expiry of the 3-month deadline, the whistleblower must be informed of this along with information on when further feedback can be expected.

As mentioned, a whistleblower can choose to come forward, and in that case it may be relevant, for example, to have physical meetings with the Recipient.

## 2.11 Confidentiality

The whistleblower scheme is designed and managed in such a way as to ensure the confidentiality of the identity of the whistleblower and any persons who may be mentioned in a report.

The Recipient is subject to a duty of confidentiality, and access restrictions have been put in place for all information relating to a report.

## 2.12 Registration of reports

Received reports, including the documents included in a report, must be registered (stored systematically) to ensure that the reports are accessible and that, if applicable, they can be used as evidence in any subsequent trial. At the same time, the registration also provides assurance that any reports concerning the same matter are identified and can lead to further investigation of a matter. This registration takes place in the whistleblower system.

Reports are retained for as long as necessary and proportionate. The principles of retention are described in more detail in IATS's privacy policy regarding the whistleblower scheme.

## 2.13 Rights of persons concerned

Any person mentioned in a report has the right to have their identity protected in connection with the processing of the case. In addition, the affected persons must have access to an effective defence, which is ensured i.e. by registering a report and thus ensuring documentation of the matters mentioned.

The persons concerned also have a number of rights in connection with the processing of their personal data. However, IATS's duty of confidentiality entails restrictions in relation to when persons concerned should receive information about the processing of information, and in relation to whether they can invoke right of access, erasure, etc.

If a report leads to a case being brought, the person the report concerns has the right to a consultative procedure or the right to access records concerning the information included in a report. However, if the whistleblower is anonymous, there is no right of access regarding the whistleblower's identity.

## 2.14 External whistleblower scheme

As an alternative to the IATS Whistleblower Policy, the National Whistleblower scheme (<https://whistleblower.dk/english>), may be used as an alternative.

IATS's employees have freedom of choice regarding whether to report to IATS's internal whistleblower scheme or the above alternative scheme. However, IATS encourages its employees to use IATS's own whistleblower scheme in cases where the employee believes that the suspected violation can be handled effectively internally and there is no risk of retaliation.

The option to use either the internal or the external whistleblower scheme does not limit employees' usual freedom of expression.

## 2.15 The whistleblower's right of publication

The Whistleblower Directive and the protection the rules give to whistleblowers also apply to a whistleblower's publication of information mentioned in a report.

However, it is a prerequisite that the whistleblower

- has, prior to publication, made a report both to the IATS internal whistleblower scheme and to an external whistleblower scheme without any appropriate action being taken, or
- has reasonable grounds for believing that the violation in question constitutes an imminent or obvious danger to the public interest, or
- has reason to believe that reporting to the external whistleblower scheme will entail a risk of retaliation, or that the case will not be dealt with effectively due to its specific circumstances.