

ISS GROUP

# ISS Speak Up Policy

Group Legal



# ISS Speak Up Policy

## Table of Contents

1. Policy Statement	2
2. Scope – what to report in the Speak Up system	3
3. What not to report in the Speak Up system	3
4. How to report concerns covered by the Speak Up Policy	3
5. Confidentiality – communication via the Speak Up system	4
6. Protection – no retaliation against reporters	4
7. Investigation process	4
8. Possible outcomes of the Speak Up report	5
9. Alternative Reporting Options: reporting to authorities	5
10. Processing of personal data	5
10.1 The types of personal data processed by ISS	5
10.2 The legal basis for processing	6
10.3 The recipients of the personal data	6
10.4 Transfer of personal data to third countries	6
10.5 Your data protection rights	7
11. Retention of the records	7
12. Contact details	7

### Our purpose:

*Connecting people and places to make the world work better*



## 1. Policy Statement

In line with the ISS Values and Code of Conduct, the business integrity of ISS is non-negotiable. ISS is committed to conducting our business in accordance with the law and high ethical standards.

This policy aims to:

- provide a platform for employees, business partners and other stakeholders to raise concerns covered by ISS policies and other breaches of applicable legislation, including the EU Whistleblower Directive,
- ensure that such concerns are treated seriously and appropriately, and
- re-assure that any person raising a concern in good faith will be protected from reprisals or retaliation.

If you wish to report a concern within the scope of the Speak Up Policy, you can report the matter by accessing the ISS whistleblower system (the “Speak Up system”):

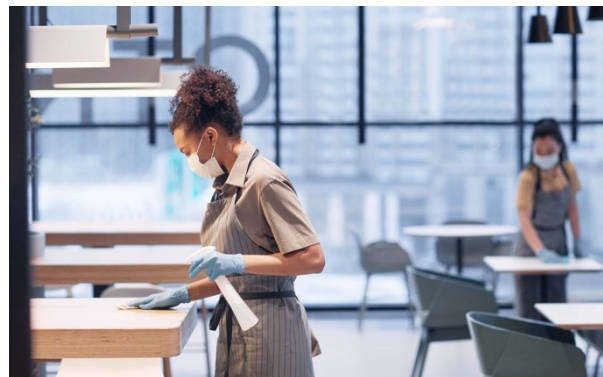
<https://iss.whistleblownetwork.net/>

## 2. Scope – what to report in the Speak Up system

The Speak Up system is meant to provide a secure and confidential channel for reporting suspected misconduct, possible breach of regulations or internal policies or concerns that could have an adverse impact on the reputation, operations and performance of the business of ISS and which, due to the nature of the concern, cannot be reported through the normal reporting lines.

The nature of concerns could include:

- unlawful activity, e.g. criminal acts such as breaches of non-disclosure obligations, abuse of funds, theft, fraudulent misrepresentation, embezzlement, fraud, and bribery;
- financial fraud, e.g. accounting manipulation, non-compliance with internal control procedures, misappropriation of assets, or fraudulent statements;
- bribery or corruption, e.g. conflicts of interest, bribery, sponsorships, donations, gifts, or facilitation payments;
- serious acts by senior management that cannot be reported using local channels without risk of adverse impact;
- violation of competition laws, e.g. price fixing, exchange of price sensitive information or collusion with competitors;
- serious endangerment to environment, health or safety, including food safety;
- activities, which otherwise by law, treaty or agreement, amount to serious improper conduct, e.g. discriminatory practices, sexual harassment, use of child labour, or human rights violations;
- breaches within other areas as defined by the EU Whistleblower Directive, e.g. public procurement, money laundering and terrorist financing, product safety and compliance, public health, data protection and information security violations.



## 3. What not to report in the Speak Up system

Concerns relating to your employment terms or local workplace matters such as conflicts with colleagues and managers, disciplinary sanctions, correct and timely payment of wages and benefits are outside the scope of the Speak Up Policy and should normally be reported to your local superior or the local Head of People & Culture and be resolved locally.

If you are not comfortable addressing your concern within the local reporting lines or the matter is not resolved satisfactorily, please use the Speak Up system for reporting your concern.

## 4. How to report concerns covered by the Speak Up Policy

If you wish to report a concern within the scope of the Speak Up Policy, you can report the matter by accessing the Speak Up system on our corporate website <https://www.issworld.com/about/corporate-responsibility/responsible-business-conduct-and-speak-up>.

The Speak Up system allows for submission of written reports as well as oral reports by the phone hotline. You can report in multiple languages. Please note that when reporting a case by phone hotline, you may experience waiting time before an agent and/or translator is available to take your call.

You are always welcome to report a concern in confidentiality to the Head of Group Internal Audit (please see contact details below).

## **5. Confidentiality – communication via the Speak Up system**

When you register a report, the system does not log the IP address of the computer or mobile device that you use and does not use cookies.

All communication will be anonymous and confidential unless you instruct otherwise. To facilitate investigation of the matter, you are encouraged to identify yourself and explain your concern in sufficient detail. Follow-up questions and investigation may not be possible unless the source of the information is identified. To assist ISS with the investigation, please provide as much information as possible.

When a report is submitted through the Speak Up system, you can choose to establish an anonymous mailbox in the system for communication purposes. ISS may in such case use this communication channel for follow-up inquiries, further dialogue and feedback, where relevant. You can edit or supplement your report by use of the mailbox or directly in the system by use of a given case number and password. You may choose to close the communication channel at any time.

ISS will treat all concerns raised under this Policy in a confidential manner except to the extent necessary to conduct a complete and fair investigation. Your identity will be kept confidential and will in general not be shared with persons outside the investigation team. Should sharing of your identity under the circumstances be necessary, we will seek your consent to do so, unless it is specifically, legally permitted not to involve you.

## **6. Protection – no retaliation against reporters**

If you report a concern to ISS in good faith, we will ensure that there will be no discriminatory or retaliatory action against you as a result of a Speak Up report.

National laws, where applicable and relevant, that may provide better protection for you as a result of the Speak Up report and investigation, will supplement or override this Policy.

Retaliation means any direct or indirect act or omission which causes or may cause unjustified detriment to the reporter. If you believe you have been retaliated against for reporting or participating in an investigation, you should immediately report such perceived retaliation to the Head of Group Internal Audit (please see contact details below) or

by using the Speak Up system. All such reports will be investigated confidentially.

However, you will not be entitled to protection if you report in bad faith, deliberately report inaccurate information or information about breaches that are manifestly unfounded. In addition, this Policy does not prohibit adverse action taken against employees for legitimate, non-retaliatory reasons.

## **7. Investigation process**

The Speak Up system and the investigation process is designed to ensure independence and absence of conflict of interest.

Your concern will be received via the dedicated Speak Up system hosted by an external provider and screened by an external law firm to safeguard the process from conflicts of interest, before sending the report to the Head of Group Internal Audit or escalating it to appropriate ISS bodies. The Head of Group Internal Audit shall (i) record and acknowledge within 7 days all reports, (ii) consider the seriousness and credibility of the report raised and (iii) proceed accordingly in determining the appropriate action. Some reports may be resolved without requiring investigation. Reports are forwarded via the Speak Up system where all communication and storage of personal data take place in an encrypted form and are password protected.

The Head of Group Internal Audit may consult your report with the ISS Business Integrity Committee or the ISS Audit & Risk Committee and any senior members of management. The Head of Group Internal Audit may also engage external auditors, investigators and/or legal counsel to assist in the investigation and analysis of the results.

The conclusions of the investigation will be submitted to the Audit & Risk Committee. The Audit & Risk Committee may decide on placing any investigation report before the Board of Directors depending on the gravity and magnitude of the violation.

ISS will give you feedback on your report within a reasonable timeframe not exceeding 3 months from the date of acknowledgement of receipt.



## 8. Possible outcomes of the Speak Up report

Appropriate remedial action will be taken in case an investigation shows violation of ISS policies and/or laws and regulations.

Where legally possible and depending on the circumstances, ISS will inform you of the action envisaged or taken as follow-up to the report and the reasoning for that follow-up.

A report will generally not have any consequences for the persons concerned if the allegations are not supported by evidence or by the outcome of the investigations.

## 9. Alternative Reporting Options: reporting to authorities

If you reside in the EU, you may - instead of reporting to ISS - report a concern to the local external reporting channel available in your country. The external reporting channel is managed by a local authority in your country permitting reporting similar to reporting internally to ISS.

For information on which authority is managing the external reporting channel, please check the [Responsible Business Conduct & Speak Up webpage](#). In Denmark, the external whistle-blower reporting channel is the Danish Data Protection Agency.

You are encouraged to report concerns to ISS first.

## 10. Processing of personal data

Collection, processing, and any disclosure of personal data submitted via the Speak Up system will be carried out in compliance with applicable data protection laws, including the General Data Protection Regulation ("GDPR") and the Danish Data Protection Act.

### 10.1 The types of personal data processed by ISS

Unless the report is submitted anonymously, the report will involve processing of personal data about you as well as the person(s) concerned and other individuals mentioned in the specific report.

The individuals in question will be notified when a report is received, and an investigation is initiated, unless the notification needs to be postponed to ensure an effective investigation or if there are other material and justified interests of ISS, which outweigh the interests of the individual(s) being investigated.

The personal data processed as part of a report will be name and contact details as well as a description of the matter/incident which led to a report, including potentially a criminal offense under the applicable laws.

The examination of a reported matter may involve collection and processing of additional information, including information gathered via conversations with you, the person concerned, the employees and board members, business partners, shareholders, or other stakeholders involved, where relevant and appropriate. The processing may also include information on potential sanctions under the employment law as well as content of any relevant notifications to authorities, including police reports.





## 10.2 The legal basis for processing

If the report is covered by the scope of the Danish Whistleblower Act, the legal basis for the processing of any categories of personal data with regards to that report is section 22 of the Danish Whistleblower Act.

In other cases, the processing of ordinary personal data in respect of any (potential) violation is based on ISS's legitimate interest to investigate a relevant matter and maintain an independent whistleblower system where an incoming report can be received and processed in line with the standards determined by ISS and reflecting our values, cf. Article 6(1)(f) of the GDPR. Processing of any personal data relating to criminal convictions and offences will be carried out in accordance with Article 10 of the GDPR (and if relevant Section 8(3) and (4) of the Danish Data Protection Act).

If in exceptional cases, special categories of personal data are processed (sensitive personal data), the legal basis for the processing of such personal data will be Article 9(2)(f) or (g) of the GDPR.

Any relevant disclosure of personal data to public authorities, including the police, will be based on a legal obligation to disclose such information and/or ISS's legitimate interest to report relevant violations to the authorities. Such disclosure will be carried out pursuant to applicable data protection laws, including the GDPR and the Danish Data Protection Act.

The processing of personal data as part of a sanction pursuant to employment law, which is derived from a report, will be based on ISS's legitimate interests, such as consideration of our business and reputation as well as maintaining the standards for working within the ISS Group.

## 10.3 The recipients of the personal data

The personal data collected via the Speak Up system may be disclosed to the relevant entities within the ISS Group, public authorities as well as third parties involved in the processing of the incoming reports. Such third parties are data processors acting on behalf of ISS and they may only process personal data subject to a data processing agreement and upon instructions from ISS. Such disclosure will be carried out pursuant to applicable data protection laws, including the GDPR and the Danish Data Protection Act.

## 10.4 Transfer of personal data to third countries

In certain situations, your personal data may be transferred to a country outside of EU/EEA. In such case ISS ensures an adequate level of security by transferring to countries approved by the EU Commission as having an adequate level of protection, or by entering into the EU-Commission's standard contractual clauses with the non-EU/EEA entity receiving the personal data, including ensuring any relevant supplementary safeguards if deemed relevant. If you wish to obtain a copy of the appropriate safeguards provided for the transfer of personal data to third countries, please contact the Group Data Protection Manager (please see contact details below).

## 10.5 Your data protection rights

ISS has taken all necessary and adequate steps to protect the reporters as well as the persons concerned and their personal data and ensure their rights as a data subject.

As a data subject you have several rights in accordance with the data protection laws. Please note that certain limitations may apply to your ability to exercise these rights, for example, when your right to obtain the information is found to be overridden by essential considerations of private interests. Subject to such limitations the following rights may be exercised:

- Right of access, e.g., you have the right to request access to your personal data and receive a copy of the personal data.
- Right to rectification, e.g., you have the right to rectify inaccurate personal data concerning you, including completion of incomplete personal data.
- Right to erasure - under certain circumstances, ISS is obliged to erase the personal data processed concerning you upon your request.
- Right to restriction - under certain circumstances, you have the right to restrict our processing of personal data concerning you.
- Right to data portability - where processing is based on your consent or performance of a contract with you, you have the right to receive the personal data concerning you in a structured, commonly used and machine-readable format and transmit these personal data to a third party.
- Right to object - under certain circumstances, you have the right to object to our processing of your personal data.

If processing of your personal data is based solely on your consent, you may withdraw your consent at any time. Please note that this does not affect our processing of your personal data prior to the withdrawal of your consent.

If you wish to exercise any of the rights, please contact the Group Data Protection Manager (please see contact details below).

You and the person concerned may at any time lodge a report with the relevant supervisory authority. In Denmark, the supervisory authority is the Danish Data Protection Agency ([www.datatilsynet.dk](http://www.datatilsynet.dk)).

## 11. Retention of the records

Reported concerns will be stored only as long as it is necessary and proportionate for the purpose of complying with the applicable legislation. Accordingly, your report will be kept only as long as it is necessary to ensure documentation for any claims raised under the applicable laws, including the need of reporters and persons concerned to preserve evidence and ISS' obligation to follow up on reports received and linking reports to previous ones.

Furthermore, ISS may retain a copy of all reports, investigation reports and all relevant documentation thereof as long as necessary for the processing and documentation of the report in question.

Personal data collected via the Speak Up system will be deleted or permanently anonymized if the reported conduct is outside the scope of the Speak Up Policy or obviously unfounded. Deletion will otherwise take place when the personal data no longer serves a purpose for the investigation, or the investigation has been finalized, or for the purpose of complying with legal obligations. If authorities have been notified, the personal data will be deleted or permanently anonymized after the case is no longer investigated by the authorities.

## 12. Contact details

### POINT OF CONTACT REGARDING THIS SPEAK UP POLICY

Head of Group Internal Audit  
Email: [issgi-speakup-all@group.issworld.com](mailto:issgi-speakup-all@group.issworld.com)  
Phone: +45 3817 0000

Ordinary mail to the following address:

Head of Group Internal Audit, ISS A/S, Buddingevej 197, DK-2860 Soeborg, Denmark

### POINT OF CONTACT CONCERNING PERSONAL DATA

Group Data Protection Manager  
Email: [dpm@group.issworld.com](mailto:dpm@group.issworld.com)

Ordinary mail to the following address:

Group Data Protection Manager, ISS A/S, Buddingevej 197, DK 2860 Soeborg, Denmark

# The ISS Values

## Unity

We trust each other and believe in creating equality, inclusion and a sense of belonging for all – a culture where everyone can be their authentic selves. That includes building diverse talent and teams, creating space for collaboration, as well as leaning on and learning from one another. We know that when we act together, we deliver a better experience for our customers and their communities. Only together and united, can we deliver on our purpose.

## Honesty

At ISS, we have a proud heritage of fairness, equality and inclusion. Every day, we strive to create a culture of open communication and collaboration, where differences and individual contributions are respected and celebrated.

## Responsibility

The health and well-being of our people and those we serve is our number one priority. We want our people to be happy, to feel valued and to thrive. This means putting all our efforts into creating safe and nurturing working environments and enhancing the communities we work within.

## Entrepreneurship

At ISS, we lead by example. That means empowering people to act and innovate, suggesting improvements and better ways of working and calling out behaviour which undermines our values. Our people know they are empowered to do the right thing.

## Quality

Our people are part of one big global family that all share the same purpose – connecting people and places to make the world work better. We provide a skilled, empowered and motivated workforce who seek to deliver the highest standards 24/7, 365 days a year.

To ensure good corporate governance ISS has adopted a number of compliance policies and standards some of which can be found [here](#).

ISS has adopted a Speak Up Policy to provide a secure and confidential channel for reporting concerns.

The Speak Up Policy is available [here](#) (EN) and in other languages [here](#). If you want to learn more about the Speak Up go to Responsible Business Conduct & Speak Up [here](#).

If you are an employee, customer, business partner or other stakeholder and believe there is a breach of the ISS Code of Conduct, our policies or relevant laws and regulations, we encourage you to speak up and report this.

Depending on the nature and seriousness of the concern, you can address your concern first with your supervisor or manager, local Head of People & Culture, local Legal Director, or local CFO.

The Speak Up system is hosted by an independent third-party. The Speak Up system can be accessed through your local company website in your local language as well as on the Group ISS World Services website [here](#).

## YOU CAN ALSO DIRECTLY CONTACT

### Head of Group Internal Audit

ISS World Services A/S  
Buddingevej 197, DK-2860 Søborg, Denmark  
Email: [issgi-speakup-all@group.issworld.com](mailto:issgi-speakup-all@group.issworld.com)  
Phone: +45 3817 0000

All inquiries will be treated confidentially and in accordance with the Speak Up Policy.

## DOCUMENT CONTROL

Document version: 2.0  
Document location: <https://opf.issworld.com/policies-standards/group-legal/regulatory-compliance/speak-up-policy>  
Last updated: April 2022  
Approved by: Executive Group Management and Board of Directors  
Responsible: Group Legal  
Next review: April 2023