

# Nordic Investment Opportunities A/S

## Policy for Whistleblowing

## 1. Purpose & Scope

The Danish Act on Alternative Investment Fund Managers, cf. Consolidated Act No. 1047 of 14 October 2019 (the "AIFM Act"), section 27 a, requires that Nordic Investment Opportunities A/S (hereafter "NIO") has an appropriate reporting system to receive and handle reports ("Whistleblowing") from employees, suppliers or customers regarding suspected breaches of the regulations that applies to the NIO and other types of serious internal misconduct.

The scope of this Policy is to define the requirements applicable to the Whistleblower procedure, ensuring that all employees, suppliers or customers of NIO are able to anonymously report serious incidents without having to fear repercussions, retaliation or harassments from other employees or the management.

The requirements according to this Policy are applicable for employees, suppliers or customers of NIO and shall be used whenever an employee, a supplier or a customer wishes to report a serious breach or misconduct within NIO.

## 2. Definitions

"Whistleblowing" shall, in this Policy, be interpreted as a situation in which employees, suppliers or customers reports a serious breach of internal and/or external regulation or another form of serious misconduct using the procedure set out in this Policy and with the aim to inform the Whistleblowing function of the breach or misconduct.

Serious breaches and misconduct may include activity that is deemed illegal, unethical or incorrect in accordance with NIO's internal regulations as well as external regulations. Both actual and potential breaches/misconduct may be reported. It may not always be obvious that a serious breach or misconduct has occurred as its existence may be concealed by other employees within NIO.

What constitutes a serious beach or misconduct shall be individually determined. Whistleblowing must, however, not be used to report regular discontent and neither shall it be used as a way to spread rumors or to discredit employees within the NIO.

## 3. Protection of the Whistleblower

If an employee, a supplier or a customer of NIO reports a serious breach or misconduct by using the Whistleblower procedure or report to the Danish FSA or to the European Securities and Markets Authority, no action may be taken against such, provided he/she had reason to believe that such a breach or misconduct had occurred.

## 4. Operational requirements

All employees, suppliers or customers can anonymously report a serious breach or misconduct by accessing the following website (link can be found on NIO's website);

<https://niopartners.whistleblownetwork.net>

The employee, supplier or customer is required to give as many facts about the breach as possible. This may be facts regards to processes, requirements, people involved, It-systems used etc. The employee, supplier or customer may upload factual evidence about the breach on the website.

The web service can be accessed from any computer with internet access. Enter the relevant internet address <https://niopartners.whistleblownetwork.net> for NIO. No IP addresses or timestamps are being logged within the system

Employees, suppliers or customers who do not choose to report through the webservice shall be aware that their anonymity cannot be ensured to the same extent. The employee, supplier or customer can choose not to accept to provide NIO with further information when making a report.

Once a report is made NIO's Compliance function will review and reply to the report according to AIFM Act.

All reports will be handled with utmost precaution in order not to reveal the identity or any characteristics of the person who filed the report, the so called "Whistleblower". Breaches/misconduct will be reported to the CEO and Board, in a manner that preserves the anonymity.

If the suspicion of breach or misconduct is related to the Chairman of the Board of Directors or the Compliance Officer, the Whistleblower shall send the report directly to the CEO instead.

The Compliance function is responsible for reporting breaches to the Danish FSA or European Securities and Markets Authority, if required by law.

If the identity of the Whistleblower is revealed for any reason, no such information shall be distributed externally unless disclosure is required by national law in relation to police investigations or judicial proceedings.

The Board will annually be informed of the number of Whistleblowing reports made. The information shall be compiled by the Risk & Compliance function.

## **5. How reported breaches and/or misconduct is handled by the Compliance Function**

All breaches/misconducts that are reported to NIO's Whistleblowing account will be taken seriously. The Compliance function will rank the information in three risk categories:

Red = An acute, actual or potential breach/misconduct exists or has existed. Red breaches/misconduct will result in the Compliance function immediately investigating the breach and then reporting it to the CEO and Board of Directors, as appropriate. An action plan will be established and followed up by the Compliance function.

Yellow = The actual or potential breach/misconduct is severe but not acute. The Compliance function will investigate and then report to the CEO or the Board of Directors as appropriate. An action plan will be established and followed up by the Compliance function.

Green = What is reported is not by severe nature. The Compliance function will take notice of the reported breach/misconduct and if necessary report it to the CEO. Many "green" reports may together be considered as a yellow breach/misconduct and handled according to the above.

## 6. **Personal Data Protection**

An employee, a supplier or a customer may accept to provide further information when making a report. All personal information will be handled in accordance with General Data Protection Regulation as implemented in Danish law. Information about handling personal data must be provided on the website above.

## 7. **Responsibilities**

### 7.1 **Board of Directors**

The Board shall approve this Policy and review and approve upon changes.

### 7.2 **CEO**

The CEO is responsible for taking any necessary actions for meeting all reports made according to this Policy, as well ensure that this Policy is complied with. The CEO shall ensure that the latest version of this Policy is accessible to those that it applies to.

### 7.3 **Compliance Function**

Compliance is responsible for providing assurance of action plans being implemented for reported breaches/misconduct. Compliance shall report breaches according to this Policy

## 8. **Policy Governance**

The following states the changes made to this policy.

Version	Date of approval	Revision details
1 (AIFM)	29 April 2020	Approved by the Board of Directors