2022

VEDIKA CREDIT CAPITAL LTD

PARTNER IN THE GROWTH OF MICRO ENTREPRENEURS

WHISTLEBLOWING POLICY

1. **Font Name & Size:** Source Sans Pro, 11
2. **Version:** 2.0
3. **Prepared and/or revised by**: Human Resource Department
4. **Reviewed by**: Board of Directors
5. **Review Date**: 18.04.2022
6. **Approved by**: Board of Directors
7. **Approval Date:** 18.04.2022

VEDIKA CREDIT CAPITAL LTD
PARTNER IN THE GROWTH OF MICRO ENTREPRENEURS

Contents

1. INTRODUCTION AND PURPOSE

1.1 The purpose of the Procedure is to ensure that persons who may use the service know the procedure for reporting suspicious activities through the Company's whistleblowing system.

2. SCOPE

2.1 The whistleblowing system may be used by persons related to the Company, such as employees of the Company, members of the Executive Management and Board of Directors, auditors, lawyers, suppliers and other business partners of the Company, to report serious offences or suspected serious offences.

2.2 Offences and misconduct that cannot be reported through the whistleblowing system shall be reported through the ordinary channels of communication.

2.3 The whistleblowing system may only be used to report serious offences or suspected serious offences about persons related to the Company, such as the employees of the Company, members of the Executive Management and Board of Directors, auditors, lawyers' suppliers and other business partners of the Company.

3. RESPONSIBILITY

3.1 The Company encourages those serious offences are reported through the Company's whistleblowing hotline. However, it is emphasized that the system is a voluntary alternative to the ordinary communication channels.

Serious offences include:

- Financial crime and violation of applicable accounting rules.
- Bribery.
- Fraud.
- Forgery.
- Corruption.
- Theft.
- Violation of industrial safety rules.
- Environmental pollution.
- Sexual harassment, assault and instances in which employees materially abuse access to systems in order to obtain information about co-workers or others when it is not work-related.
- Violation of applicable legislation, regulations or other rules applicable the

Company's business.

- Violation of internal rules provided that:
    - the violation may lead to serious, recurring security risks;
    - the violation may lead to serious financial risks;
    - the violation may lead to regulatory measures;
    - the violation may lead to a serious qualification from the auditor; or
    - the violation may seriously damage the Company's relations with employees or external parties.

3.2 Reports to the whistleblowing hotline are screened by two partners at Plesner Advokatpartnerselskab ("Plesner"). Upon screening of the report and assessment of who at the Company should receive the report for further processing, the report is forwarded in accordance with sections 4.3 - 4.5

3.3 Subject to the conditions in 4.3 - 4.5, reports are handled by the chairman of the Audit Committee. The General Counsel and the head of Group HR may be involved

3.4 Persons who have reported breaches by use of the whistleblowing system will not be subjected to adverse treatment or adverse consequence as a result.

4. THE PROCEDURE

4.1 **Reporting Channel:**

Reports are filed via "Plesner Whistleblowerordning" found on the Company's intranet.

4.2 **Anonymous reporting:**

The Company always encourages that the reports are filed in the individual's own name, so that the persons handling the case may have the opportunity to ask additional questions and subsequently inform about how the investigations will proceed. However, it is possible to file an anonymous report.

4.3 **Appointment of the Investigator:**

When the report is filed, Plesner will on behalf of the Company forward the report to the Investigator.

The Investigator is by default the chairman of the Audit Committee. If a report concerns the chairman of the Audit Committee or any other member of the Audit Committee, Plesner will instead forward the report to the Chairman of the Board of Directors.

4.4 **Self-obligation to ensure impartiality:**

In any case, the Investigator is required - autonomously - to ensure that the report does not concern them and the reported content generally can be processed within the scope of the whistleblowing system, see section 3.1.

4.5 **Obligation to investigate:**

All reports must be investigated. However, if a reported incident is assessed to be manifestly unfounded, no further investigations shall be initiated.

4.6 **Reporting:**

Any reported matter must be closed by a written report containing a conclusion and/or recommendation for further action based on the findings of the report. The report is passed to the Company's Board of Directors. The conclusion/recommendation may be:

- The investigation has been closed as manifestly unfounded.
- The case ends with change of internal procedures.
- The case ends with a warning.
- The case ends with other disciplinary actions (expulsion/dismissal).
- The case should be filed to the police for a police investigation.
- The case should be filed with other agencies, e.g., the Danish FSA.

4.7 **Use of internal and external services:**

To the extent it is deemed absolutely necessary, the Investigator is authorized to engage internal and external assistance for the investigation of a report, including IT technical assistance, investigative and forensic assistance and legal assistance.

4.8 **Confidentiality:**

The Investigator and those individuals engaged according to section 4.7, must keep confidential all information that is received during an investigation. Until the time of the delivery of the written report to the Board of Directors, only the Investigator may authorize disclosure of information to third parties.

Information on the identity of the reporter, if known, can only be communicated on the basis of a warrant or other act of a public authority, or if the Company's otherwise subject to a legal obligation to do so, e.g., pursuant to the anti-money laundry act.

4.9 **Notification of the reported person:**

The reported person will be notified of the investigation as soon as possible, after a preliminary investigation has taken place and all relevant evidence has been secured.

The person will - among other things - be informed about:

- The identity of the person or group of persons responsible for the investigation.
- The nature of the accusations.
- Who has had access to the report?

Further information about the rights of the reported person can be found in "VEDIKA CREDIT CAPITAL LIMITED - guidelines for reported persons"

The reported person will not receive information about the identity of the reporter unless the Company pursuant to applicable law is obligated to provide such information, see section 4.8.

4.10 **Information to the Board of Directors and/or executive board:**

The Board of Directors and/or the Executive Management may be informed about reports and investigations of severe matters.

4.11 Feedback:

The Investigator will confirm receipt of a report within 5 business days where the reporter has listed his/her contact information.

The reporter is not entitled to be furnished with information during or after the completion of an investigation. The Investigator may, in cases where it is deemed unobjectionable to provide the reporter with feedback, choose to disclose information regarding the investigation, e.g., the investigation and its findings are publicly known.

4.12 Annual report to the board

The Investigator provides an annual report to the Board of Directors based on the reports received in a calendar year. The annual report accounts generally for the extent and types of report and information about who investigated the reports and their conclusion.

5. DATA SECURITY AND DATA RETENTION

5.1 Data security

Personal data that is processed within the whistleblower system, including investigative reports, are processed securely, and only authorized personnel may access the information.

Electronic personal data is protected by use of login / password, firewall and antivirus

programmes. Personal data that is manual is stored locked.

5.2 Plesner Whistleblower system

Plesner acts as a data processor on behalf of the Company in relation to the whistleblowing system, where individuals may file reports. Plesner has implemented necessary technical and organizational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in the Danish Data Protection Act.

The Company has concluded a written agreement compliant with the requirements of the Danish Data Protection Act when using data processors and compliant with the EU General Data Protection Regulation.

5.3 Data retention

Information is deleted immediately after the closing of the matter with the authorities where a report has been filed with the police or other relevant authorities. The Company notifies Plesner when the case has been closed.

Where a disciplinary case or sanction is carried out on an employee or there are other grounds in which a continued storing of information about an employee is legitimate and necessary, information will be stored in the employee's personnel file. Information about the employee is stored up to 5 years after termination of the employment.

6. PERIODICAL REVIEW OF THE POLICY

The Policy is flexible and easy to understand and comply with by all levels of employees. The Board should review this Policy periodically but at least once in a year, so that it remains appropriate in the light of material changes in regulatory requirement with respect to the Company's size, complexity, geographic reach, business strategy, market and best governance practices.

The policy can also be reviewed as and when deemed necessary by the Top Management and amendments effected to the same, subject to approval of the Board if any, and when practical difficulties are encountered. The Top management may also review the policy on document retention to comply with any local, state, central legislation that may be broadcast from time to time

7. AMENDEMENT OF THE POLICY

The Board of Directors on its own and/or on the recommendation of the Nomination & Remuneration Committee or top management can amend this policy as and when required deemed fit. Any or all provisions of this Policy would be subjected to revision/amendment in accordance with the regulations on the subject as may be issued from relevant statutory authorities, from time to time.