WHISTLEBLOWING POLICY AND PROCEDURE

June 2022

Contents

1. Definitions

1.1 In this Procedure, the following words shall have the following meaning unless the context clearly indicates otherwise:

1.1.1 **"Board"** means board of directors of the Company, including executive and non-executive directors;

1.1.2 **"Company"** means Finclusion Group Limited with registration number 180294 GBC;

1.1.3 **"Contract"** means an agreement based on consensus between legal subjects with contractual capacity that gives rise to mutual obligations enforceable by law;

1.1.4 **"Group"** means the Company and its direct and indirect subsidiaries;

1.1.5 **"Group Entity"** means any entity within the Group;

1.1.6 **"Policy"** means this Whistleblowing Policy and Procedure.

2. Introduction

2.1. The Group is committed to good corporate governance and ethical behaviour and has the expectation that where its employees, customers, suppliers, and other stakeholders believe that if the Group, its subsidiaries, or stakeholders are not demonstrating good corporate governance and ethical behaviour, they should report their concerns.

2.2. This policy and procedure specifically provides clarity that any person can report a concern without fear of victimisation, subsequent discrimination, or disadvantage. The policy and procedure further encourages that rather than ignoring a situation or concern, that all people should, either confidentially or anonymously, report the concern. The person or party reporting the concern can be assured that wherever practical, and subject to any legal constraints, investigations will proceed on a confidential basis.

3. Purpose

3.1. The purpose of this policy and procedure is to:

3.1.1. encourage persons and parties to feel confident in raising concerns;

3.1.2. provide facilities to raise concerns; and

3.1.3. ensure that whistle-blowers are protected from possible reprisals or victimisation if the disclosure was made in good faith.

4. Scope

4.1. This policy and procedure applies to all employees at all levels, including temporary or contract workers to the Group, including all subsidiary companies, wherever located.

4.2. This policy is intended to complement any policies that address risk, fraud, and ethics within the business, in totality and does not replace such policies, but should be read in conjunction therewith. Such policies include, but are not limited to:

4.2.1. The Group AML and Fraud Policy;

4.2.2. The Group Risk Management Policy;

4.2.3 The Group Disciplinary Policy; and

4.2.4 The Group Code of Conduct.

5. Whistleblowing Safeguards

5.1. The Group is committed to its employees', customers', suppliers,' and other stakeholders' rights. It recognises that the decision to report concerns can be difficult to make. If a whistle-blower reports truthfully, the whistle-blower will have nothing to fear because the whistle-blower would be acting responsibly.

5.2. The Group will protect the whistle-blower by not tolerating any harassment, victimization, or occupational detriment (including formal and informal pressures) if the whistle-blower has raised the concern, or even a suspected incident, in good faith. Any investigations into allegations raised will, however, not influence or be influenced by any current process that may already affect an employee in terms of the companies' policies and procedures.

6. Confidentiality

6.1. All concerns raised will be treated with the strictest level of confidence and every effort will be made, subject to any legal constraints, not to reveal the identity of the whistle-blower without the whistle-blower's permission. Circumstances may, however, require that in time it may be necessary for the whistle-blower's identity to become known, for example, a person may need to be called as a witness.

7. Anonymous Reporting

7.1. This policy encourages that all disclosures are confidential, therefore, the whistle-blower's identity is known to the relevant parties, and, however, it does recognise that in certain circumstances it may be the preference of the whistle-blower to report anonymously.

7.2. Concerns raised anonymously are not easily investigated due to the inability of the investigator to request additional information, and, accordingly, will need to be considered at the discretion of the forensic investigators. In exercising this discretion, the factors to be considered include:

7.2.1. the seriousness of the issues raised;

7.2.2. the detail and amount of information provided;

7.2.3. the ability of confirming the allegation from other sources; and

7.3. It is the responsibility of the whistle-blower to ensure their own anonymity.

8. Malicious Whistleblowing

8.1. Where an allegation is made in good faith, even where it is not able to be confirmed by an investigation or is subsequently proved untrue, no action will be taken against the whistle-blower. If, however, an allegation is maliciously or mischievously made for personal gain or

otherwise, appropriate disciplinary or legal action may be taken against the whistle-blower.

9. Reportable Breaches and Concerns

9.1. Employees are encouraged to report breaches and concerns including but not limited to:

9.1.1. fraudulent and corrupt behaviour which includes the unlawful and intentional making of a misrepresentation which causes actual prejudice, or which is potentially prejudicial to another;

9.1.2. theft which includes the unlawful and intentional appropriation of movable corporeal property, including information in electronic format, which belongs to and is in the possession of another; which belongs to another but is the perpetrator's own possession; or which belongs to the perpetrator but is in the possession of another person who has a right to possess it and where such right legally prevails against the perpetrator's own right of possession;

9.1.3. activities undertaken by employees which contravene Group policies and standards;

9.1.4. cyber-crime which encompasses unauthorised access to, interception of or interference with data which can be summarised as follows:

- the intentional accessing or intercepting of any data without authority or permission to do so;
- the intentional and unauthorised interference with data in a way which causes such data to be modified, destroyed, or otherwise rendered ineffective;
- to unlawfully produce, sell, offer to sell, procure for use, design, adapt for use, distribute, or possess any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or to perform any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section of the said act;
- to utilise any device or computer program mentioned above in order to unlawfully overcome security measures designed to protect such data or access thereto; or
- to commit any act described above with the intent to interfere with access to an information system so as to constitute a denial, including partial denial, of service to legitimate users.

10. Reporting and Follow up Process

10.1. Employees are encouraged to raise breaches and concerns with their line manager or their immediate superior. This, however, depends on the seriousness and sensitivity of the issues involved and who is suspected of the breach. The following reporting channel should be used:

10.1.1. **Anonymous and confidential reporting**

10.1.1.1. An email should be sent to ethics@finclusiongroup.com

10.1.1.2. When submitting a report, the following details are required:

- Country of incident observed;
- A detailed description of the incident;
- Was management notified?
- Who was/is involved in the incident?
- When did the incident occur?
- Where did the incident occur?

10.1.1.3 Detail of how you know of the incident, being either:

- Witnessed;
- Overheard;
- Involved;
- Heard from others (Hearsay);
- Unable to state;
- Alleged victim; or
- Other

10.2. Once the report detailed in 10.1.1 above has been reviewed by the Group Internal Audit Department, matters raised may be investigated by management or through a disciplinary process and, in certain circumstances, be referred to other investigating authorities. To protect all individuals concerned, initial enquiries will be made to decide whether an investigation is appropriate and, if so, what form it should take. Some concerns may be resolved without the need for investigation. If, however, urgent action is required this may also be taken before any investigation is conducted.

10.3. Within ten (10) working days of a concern being raised, the Head of Internal Audit will either institute the necessary plans for an investigation or, where more information is required after an assessment of the provided information, either defer or close the case.

10.4. In the event that a case is deferred, the Head of Internal Audit may refer the case to the relevant authorities and institute an independent enquiry.

10.5. The Head of Internal Audit shall ensure regular follow ups are conducted with the relevant authorities and/or parties to the independent enquiry.

11. Commitment to Whistle-blowers

11.1. Only with the permission of the whistle-blower will contact between the whistle-blower and the forensic investigator take place. This contact will depend entirely on the nature of the matters raised and particularly the adequacy of the information provided. Where possible and necessary, the forensic investigator involved may require a meeting to seek further information. Such a meeting will be made with both the protection and confidentiality of the whistle-blower, being paramount. Subject to any legal constraints, the whistle-blower will be kept informed of the progress and outcome of an investigation. The Group will take steps to minimise any negative impact that a whistle-blower may experience as a result of raising a concern.

12. Policy Governance

12.1. Policy governance structure

12.1.1. Amendments to the policy may arise as a result of annual review.

12.1.2. Proposed amendments to the policy must be submitted to the Group Audit and Risk Committee for consideration and approval prior to implementation.

12.2. Ownership

12.2.1. The Group Internal Audit department has overall responsibility for maintenance and operation of this policy and maintain a record of concerns raised (in a form which does not endanger the whistle-blowers' confidentiality) and reports as necessary to the Group Audit and Risk Committee.

12.3. Maintenance of Policy

12.3.1. This Policy is maintained by the Group Head of Internal Audit.

12.4. Approval of the Policy

12.4.1. This Policy is sponsored by the Chief Executive Officer and is approved by the Board of Directors.