

**Policy Name:** Whistle Blowing Policy

**Type:** Compliance

**Owner:** Head, Risk Management & Compliance

**Approved by:** Board Audit and Risk Committee (BARC)

**Date:** March 14, 2025

**Approved by:** Board of Directors (the Board)

**Date:** March 18, 2025

**Document Number:** POL-WB-COM-010 v5

**Review Date:** Biennial review required

*This document has been classified as “Public” and has been issued strictly for the business purposes of FirstCap Limited.*

## **1 Policy Statement**

- 1.1 This document sets out FirstCap Group's ("FirstCap" or "the Group") policy on Whistle blowing ("the Policy" or "this Policy").
- 1.2 This Policy governs the reporting and investigation of improper, unethical or illegal practices or activities at FirstCap and its subsidiary, as well as the protection offered to Whistle-blowers.
- 1.3 This Policy provides the minimum standards of Whistle blowing which FirstCap Group shall comply with to ensure that Conflicts of Interest or potential Conflicts of Interest are properly and carefully handled.
- 1.4 The business of the Group is built on trust and integrity as perceived by its stakeholders, especially its clients, shareholders, regulators and law enforcement agencies.
- 1.5 An important element of trust and integrity is ensuring that FirstCap and its subsidiary conducts its business in accordance with the values and Code of Ethics that it has adopted, and in compliance with applicable laws, rules and standards.
- 1.6 FirstCap Group's reputation and organisational integrity are key requirements to operate successfully as a financial institution. Failing to meet these requirements would violate the Group's core values and business principles and may expose the Group and its employees to possible regulatory and/or criminal liability.
- 1.7 FirstCap Group's Whistle blowing Policy is designed to comply with applicable statutory and regulatory obligations, ensuring that:
- 1.7.1 The Policy contains mechanisms, including assurance of confidentiality and protection that encourage all stakeholders to report any unethical practice or activity to the Group and/or the Securities and Exchange Commission. In

addition, the Group's whistle-blowing mechanism shall include a dedicated "hotline" or e-mail system, which shall be used anonymously to report unethical practices or activities.

- 1.7.2 The relevant statutory and regulatory obligations are complied with;
- 1.7.3 The Policy is exposed to employees and other stakeholders, including shareholders, contractors and the public.
- 1.7.4 Improper, unethical and inappropriate behaviour at all levels is identified and challenged;
- 1.7.5 The Group promotes and develops a culture of openness, accountability and integrity;
- 1.7.6 The Group provides clear procedures for reporting and handling improper, unethical and inappropriate behaviour.
- 1.7.7 FirstCap Group and its employees are protected from reputational damage and administrative penalties that may be imposed by various regulatory and legislative authorities because of non-adherence with this Policy and/or regulatory requirements regarding whistleblowing.

## **2 Applicability**

- 2.1.1.1 This Policy applies to all employees and directors of FirstCap and its subsidiary, including independent consultants, interns and secondees.
- 2.2 This Policy reflects the minimum requirements for the FirstCap Group.

### **3 Policy Requirements**

#### **3.1 Scope**

3.1.1 The Policy covers Concerns about actual or suspected irregularity or misconduct of a general, operational or financial nature within FirstCap Group, including but not limited to:

3.1.1.1 Accounting, internal accounting controls or auditing matters;

3.1.1.2 Money Laundering or Terrorism Financing;

3.1.1.3 Market abuse;

3.1.1.4 Insider trading/Insider abuse;

3.1.1.5 Breach of (client) confidentiality;

3.1.1.6 Theft;

3.1.1.7 Fraud;

3.1.1.8 Bribery or corruption;

3.1.1.9 Actions detrimental to Health, Safety or the Environment;

3.1.1.10 Failure to comply with regulatory directives, administrative or internal policy and/or framework;

3.1.1.11 Failure to comply with legal obligations or laws;

3.1.1.12 Non-disclosure of interest;

3.1.1.13 Connected transactions;

3.1.1.14 Sexual or physical abuse of any employee, client, job applicant, service provider or any other relevant stakeholder;

- 3.1.1.15 Corporate governance breaches;
  - 3.1.1.16 Improper conduct or unethical behaviour;
  - 3.1.1.17 Any form of criminal activity; and
  - 3.1.1.18 Any act or action carried out to conceal the above listed acts.
- 3.1.2 Complaints for which specific procedures have been established, for example, personal grievances of employees or certain types of labour law matters are excluded from the scope of this Policy.
- 3.2 **Anonymity**
- 3.2.1 FirstCap will:
- 3.2.1.1 Respect and protect the confidentiality of a whistle blower's identity, as well as the confidentiality of the details of the report or Concern, if the report is or disclosure was made in accordance with the process set out in this Policy. The Group will maintain the confidentiality of the whistle blower's identity, unless:
- I. Such a person agrees to be identified;
  - II. Identification is necessary to allow the Group or a Relevant Authority's official to investigate or respond effectively to the report or disclosure;
  - III. Identification is required by law or under the Group's policy, where a false accusation has been maliciously made; or
  - IV. The person accused is entitled to the information as a matter of legal right or under the Group's policy in the disciplinary proceedings. In such an eventuality, the Group shall inform the whistle blower prior to revealing his or her identity.

3.2.1.2 Provide each potential whistle-blower easy and anonymous access to the Designated Officer.

3.2.1.3 Provide a dedicated “hotline” and e-mail address, which employees may use to anonymously report unethical practices or other Concerns. Refer to **Annexure B** for details.

3.2.2 An employee, including senior management and the Designated Officer, must never attempt to discover the identity of a whistle-blower who has chosen to remain anonymous;

### 3.3 **Anonymous Access**

3.3.1 FirstCap encourages whistle blowers to disclose their identity when reporting to make their reports more credible.

3.3.2 However, if the whistle blower only feels able or comfortable to report a Concern if made anonymously, then the whistle blower can report the Concern anonymously. The whistle blower should take the below factors into consideration when deciding whether to disclose his or her identity or remain anonymous:

3.3.2.1 The seriousness of the Concern;

3.3.2.2 The significance and credibility of the Concern; and

3.3.2.3 The possibility of confirming the allegation.

### 3.4 **Whistle blower Protection**

3.4.1 The Group will protect whistle-blowers against retaliation. Whistle blowers’ reports will be handled with sensitivity, discretion and confidentiality. Any report of retaliation, including but not limited to, any act of discrimination, threats of physical harm, loss of job (in the form of dismissal, termination or redundancy), demotion, punitive work assignments, withholding of benefits

and/or entitlements, reprisal, harassment, vengeance or reduced salary or wages, will be promptly investigated and corrective action taken, where allegations are substantiated.

3.4.2 The Group shall ensure that a whistle blower, or any employee who provides information, who causes information to be provided or who otherwise assists in an investigation, is protected from retaliation. Specifically, the Group shall ensure the protection of Whistle blowers by:

3.4.2.1 Strictly prohibiting Retaliation. The Group unequivocally prohibits retaliation, in any disguise, against any whistle blower who blows the whistle in good faith;

3.4.2.2 Educating its employees on the requirements of this policies, including the specific prohibitions; and

3.4.2.3 Subjecting to disciplinary action, civil action or criminal prosecution, any employee who retaliates or attempt to retaliate against a whistle blower or against any employee who provides information, who causes information to be provided or who otherwise assists in an investigation.

3.4.3 Any employee or a member of the public, who suspects to have been, or who in fact, has been retaliated against, in violation of this Policy, must report immediately to a Designated Officer.

3.4.4 Whistle blowers must ensure that they do not report or make disclosures outside of prescribed channels (for example, going to the media), or their report or disclosure may not be protected.

### 3.5 **Confidentiality**

3.5.1 Protected reporting may be made on a confidential basis by the whistleblower. Protected reporting and investigatory records will be kept confidential to the extent possible, consistent with the need to conduct an adequate investigation and to report results to Relevant Authorities as may be required

by law or regulation. In case the Group decides to refer an incident under investigation to a law enforcement agency, the Group reserves the right to do so without obtaining the consent of the employee(s) involved in the incident.

3.5.2 A whistle blower is encouraged to report and provide new or additional details of the report or Concern to the Designated Officer only. The Designated Officer is responsible for forwarding new or additional details to the appropriate Authorised Persons on a strict “Need to Know” basis.

3.5.3 Neither a whistle blower nor any other employee who provides information, who causes information to be provided or who otherwise assists in an investigation is allowed to discuss the details of the reported Concern or any related investigation with anyone except the Designated Officer, unless specifically requested to do so by the Designated Officer or required by law and/or regulation (e.g. in a regulatory investigation or court hearing). In such cases, the whistle blower’s contribution does not affect the whistle blower’s rights and protection under this Policy, nor does it change any of the obligations as mentioned in this Section (Section 3.5).

3.5.4 An exception to the confidentiality principle is when FirstCap Group is required by law or regulation to disclose information related to a whistle blower’s Concern, including the whistle blower’s identity and/or the identity of the accused person(s), to an external party who is legitimately authorised.

### 3.6 **Whistle blowers’ Rights**

Whistle blowers have the right to:

3.6.1 Have easy and anonymous access to a Designated Officer; and

3.6.2 Have their identity kept confidential.



### 3.7 **Obligations of FirstCap Group**

FirstCap Group must:

- 3.7.1 Provide each potential whistle blower easy and anonymous access to a Designated Officer;
- 3.7.2 Protect from retaliation a whistle blower, or any employee who provides information, who causes information to be provided or who otherwise assists in an investigation;
- 3.7.3 Respect and protect the Confidentiality of a whistle blower's identity as well as the confidentiality of the details of the Concern;
- 3.7.4 Appoint a Designated Officer. This appointment must be approved by the Board;
- 3.7.5 Ensure publication and easy access on the intranet of the appropriate contact details of the Designated Officer(s);
- 3.7.6 Provide a dedicated "hot line" and e-mail address as well as the e-mail address of the Securities and Exchange Commission (SEC), if any, as alternative channels to report Concerns. There is currently no e-mail address for reporting Concerns to the SEC;

### 3.8 **Whistle blowers' Obligations**

Whistle blowers must:

- 3.8.1 Consider using normal reporting channels before reporting a Concern under this Policy. Specifically, the recommended **reporting channels** in order of preference are as follows:

- 3.8.1.1 Employees are encouraged to report any Concerns through the normal reporting channels (i.e. through their immediate line manager, head of department or higher-level manager) in order to keep an open dialogue;
- 3.8.1.2 If an employee feels unable or uncomfortable raising the Concern through the normal reporting channels, the employee is then encouraged to report the Concern to the Group's Designated Officer. As such, this Policy complements the normal reporting channels;
- 3.8.1.3 If an employee feels unable or uncomfortable raising the Concern to the Group's Designated Officer, the employee is then encouraged to report the Concern by using an internal alternative channel.
- 3.8.2 Consider using the internal alternative channels before using an external alternative channel;
- 3.8.3 Report Concern in good faith;
- 3.8.4 Provide all relevant information;
- 3.8.5 Be available to the Designated Officer for an investigation; and
- 3.8.6 Respect confidentiality.

### 3.9 **Making Information Available to the Designated Officer**

- 3.9.1 Whistle blowers are requested to provide information at hand and any known details about the event(s) underlying the Concern, such as:
  - 3.9.1.1 The date of the event(s);
  - 3.9.1.2 The nature of the event(s);
  - 3.9.1.3 The name of the person(s) involved in the events;
  - 3.9.1.4 Possible witnesses to the event(s); and

3.9.1.5 Evidence of the event(s), e.g. documents, e-mails or voice recordings/loggings.

3.9.2 Whistle blowers must meet any reasonable request to clarify any facts and/or circumstances, to provide (additional) information and to cooperate with an investigation. A lack of information can be the reason for deciding not to investigate and/or to conclude that the Concern has no factual basis.

### 3.10 **False Allegations**

3.10.1 Any employee who knowingly, with reckless disregard for the truth or decides to, in bad faith, gives false information or makes a malicious report of wrongful or unethical conduct may be subject to disciplinary action, up to and including termination of employment.

3.10.2 This Policy is not intended to be utilised for the reporting of petty disputes, grievances, false or misleading disclosures, matters currently under disciplinary enquiry and matters already pending before the Courts.

### 3.11 **Denial of the Right to Immunity**

3.11.1 Whistle blowers reporting a Concern whose own conduct is implicated in the Concern will not be given any automatic immunity from investigation, disciplinary action, criminal prosecution and/or civil liability.

3.11.2 The same applies to any other employee who provides information, who causes information to be provided or who otherwise assists in an investigation.

### 3.12 **The Designated Officer**

3.12.1 The Head, Internal Audit Department has been appointed as the Designated Officer to be a point of contact for concerns raised under the Whistle-blowing Policy. The Designated Officer is expected to, always, be impartial and capable of taking an independent view on the Concern raised. The Designated Officer shall, from time to time, advise employees of the whistle blowing “hotline” and

e-mail address of the Group for anonymous reporting. This information must be made public via the Group's website. Refer to **Annexure A** for the details of the Designated Officer.

3.12.2 The responsibilities of the Designated Officer shall include, but not limited to, the following:

3.12.2.1 The review of reported cases;

3.12.2.2 Recommendation of appropriate actions to the MD/CEO and where issues affect Executive Management, such issues should be referred to the Board.

3.12.2.3 Carry out further actions based on the recommendation;

3.12.2.4 Provide a report to the Board Audit and Risk Committee (BARC) with summary of cases reported and the result of the investigations conducted on those cases.

### 3.13 **How to Report (The Reporting Process)**

The reporting process is as documented in **Annexure C**.

### 3.14 **Investigation (The Investigation Process)**

The investigation process is as documented in **Annexure D**.

### 3.15 **Record Keeping**

3.15.1 FirstCap shall maintain a record of all activities, reports and information received pursuant to this Policy for a minimum of 10 years. Such records may include initial contact reports, transcripts from meetings and verbal conversations about the (alleged) Concern and all facts from an investigation.

3.15.2 All whistle blowers' records must, as a minimum, be classified and handled as "Confidential."

3.15.3 Notwithstanding the foregoing, the recording and retention of all Full investigation must be done in accordance with the Group's Policy.

### 3.16 **Waiver**

None of this Policy's principles or provisions can be waived.

### 3.17 **Deviations**

3.17.1 Any deviations from this Policy because of applicable law or regulation must be incorporated into applicable procedures.

3.17.2 Only deviations from this Policy required or necessitated by applicable law and/or regulation are permitted.

3.17.3 The Designated Officer must document in his or her report to the Board Audit Committee, any deviations to any principle laid down in this Policy and its consequences.

3.17.4 The Designated Officer must also inform the Head of Compliance of such deviations and likely consequences.

## **4 Roles and Responsibilities**

### 4.1 **FirstCap Board of Directors**

4.1.1 Has ultimate responsibility for this Policy;

4.1.2 Has the responsibility to establish a whistle blowing mechanism for reporting illegal and unethical behaviour; and

4.1.3 Initiates disciplinary action required for any breach of this Policy by a Director.

### 4.2 **FirstCap Board Audit and Risk Committee**

4.2.1 Adopts and approves this Policy;

- 4.2.2 Supports the implementation of this Policy;
- 4.2.3 Reviews reports on non-compliance with this Policy;
- 4.2.4 Reviews the report of the summary of significant cases and the result of the investigation furnished by the Designated Officer;
- 4.2.5 Familiarises itself and adheres to the Policy; and
- 4.2.6 Institutes and maintains measures and controls to ensure adherence to this Policy.
- 4.3 **Management Committee (MANCOM)**
  - 4.3.1 Considers and approves this Policy;
  - 4.3.2 Minutes any exceptions or deviations allowed in terms of this Policy; and
  - 4.3.3 Review reports on non-compliance with this Policy.
- 4.4 **Heads of Departments/Heads of Units (collectively referred to as "HODs")**
  - 4.4.1 Familiarise themselves with and adhere to this Policy;
  - 4.4.2 Ensure that all employees in their respective Departments/Units familiarise themselves with and comply with this Policy;
  - 4.4.3 Ensure that all employees (current and new) in their respective Departments/Units are informed of the Group's Whistle blowing Policy and expectations in relation to the confidential reporting (Whistle blowing) process/mechanisms;
  - 4.4.4 Ensure any contractors, consultants or others are briefed on the requirements of this Policy; and

4.4.5 Where applicable, make formal application to the Designated Officer for any dispensations to the minimum requirements of this Policy.

4.5 **Risk Management and Compliance must:**

4.5.1 Develop, review and maintain this Policy;

4.5.2 Raise awareness in terms of this Policy;

4.5.3 Monitor adherence to this Policy and related procedures, as well as the implementation of this Policy;

4.5.4 Provide training and guidance in respect of this Policy; and

4.5.5 Advise employees, line managers and HODs, where necessary.

4.6 **Internal Audit (“The Designated Officer):**

4.6.1 Develop and maintain procedures to support the principles of this Policy;

4.6.2 Participate in the review of this Policy;

4.6.3 Review reported cases and recommend appropriate action to the MD/CEO and where issues affect Executive Directors, such issues shall be referred to the Board;

4.6.4 Advise employees of the whistle blowing “hotline” and e-mail address of the Group for anonymous reporting;

4.6.5 Develop procedures to handle investigations, feedback and reporting;

4.6.6 Provide a report to the Board Audit & Risk Committee (BARC) with summary of cases reported and the result of the investigations conducted on those cases;

4.6.7 Provide training and advice to employees on the identification and management of Conflicts of Interests and adherence to this Policy;

- 4.6.8 Investigate and identify potential Conflicts of Interest; and
- 4.6.9 Facilitate any regulatory, internal/external audit or internal investigation in respect of this Policy.
- 4.7 **Employees must:**
- 4.7.1 Familiarise themselves with and adhere to this Policy and related Whistle-blowing procedures;
- 4.7.2 Complete all relevant training on Whistle blowing;
- 4.7.3 Ensure that known or suspected breaches of this Policy are reported to Compliance and/or the Designated Officer immediately;
- 4.7.4 Co-operate with the Designated Officer for any regulatory, internal/external audit or internal investigation in respect of this Policy;
- 4.7.5 Practice honesty, transparency and integrity in fulfilling their responsibilities as contained in this Policy and as employees of FirstCap Group. The Group encourages all employees and directors acting in good faith, to report suspected or actual wrongful conduct; and
- 4.7.6 Not directly or indirectly use or attempt to use their official authority or influence of their positions or offices for the purpose of interfering with the right of an individual to make a protected disclosure in line with this Policy.

## **5 Related policies and procedures in FirstCap Group**

- 5.1 Code of Conduct and Ethics.
- 5.2 Anti-Bribery and Corruption Policy.
- 5.3 Conflicts of Interest Policy.
- 5.4 Conflicts Clearance and Deal Management Procedures.



- 5.5 Personal Account Trading (PAT) Procedures.
- 5.6 Compliance Manual.
- 5.7 Confidential Information Policy.
- 5.8 Chinese Walls Policy.
- 5.9 Confidential Information procedures.
- 5.10 Chinese Walls Management and Wall Crossing procedures.
- 5.11 Watch and Restricted List Policy and related procedures.

## **6 Disciplinary Action**

- 6.1 Failure to adhere to this Policy (either intentionally or as a result of negligence) shall result in disciplinary action, which may lead to the termination of employment.
- 6.2 Anyone who breaches this Policy may suffer personal consequences. Specifically:
  - 6.2.1 Employees, including senior management staff and the Designated Officer, who breach any of the provisions of this Policy, may be subject to disciplinary action, criminal prosecution and/or civil liability;
  - 6.2.2 A Whistle blower who has not acted in good faith by reporting an alleged Concern under this Policy, or who does not respect the Confidentiality provisions of the Policy:
    - 6.2.2.1 May lose the rights and protections provided under this Policy; and
    - 6.2.2.2 May be subject to disciplinary action, criminal prosecution and/or civil liability.

6.3 In addition, an employee may be held personally liable for civil or criminal penalties, which may include fines, payment of damages or imprisonment.

## **7 Definitions**

### **7.1 An Alternative Channel**

A channel through which a Whistle blower can report a Concern anonymously or by disclosing his or her identity.

### **7.2 Anonymity/Anonymous**

Anonymity relates to the identity of the Whistle blower. A Whistle blower is Anonymous when his or her identity is not known to any employee, including the Designated Officer.

### **7.3 Anonymous Whistle blowing**

Alternative to confidential reporting, a Whistle blower may choose not to reveal his or her identity when a report or disclosure is being made. The Group has established a Whistle blowing “hotline” and an e-mail address to aid anonymous reporting of Concerns. The hotline and e-mail address are managed by the Designated Officer.

### **7.4 Authorised Persons**

Authorised Persons are persons who are strictly necessary for the handling and/or investigation of Whistle blower’s Concern. The Designated Officer determines the persons who are/become Authorised Persons on a case-by-case basis. On a strict “Need-to-Know basis with special consideration given to potential conflicts of interest and confidentiality, Authorised Persons (could) include external consultants or investigators, employees of the Internal Audit Department, employees of the Compliance function, employees of the Legal Department and employees of the Risk Management function.

## 7.5 **Concern**

A report raised by a Whistle blower about an actual or suspected irregularity or misconduct within the Group that leads or could lead to a violation of:

7.5.1 FirstCap Group's Policies;

7.5.2 FirstCap Group's Codes;

7.5.3 Any law, regulation or Rules.

## 7.6 **Confidential/Confidentiality**

Confidentiality refers to the non-disclosure of certain information such as the identity of the Whistle-blower, the content of the Concern, as well as any other details related to the Concern and any investigation of the Concern. This also includes any information that relates to the identity of the Whistle-blower.

## 7.7 **Confidential Whistle blowing**

7.7.1 A Whistle blower may choose to reveal his or her identity when a report or disclosure is being made. Should this be the case, the Group, through the Designated Officer, will respect and protect the confidentiality of the Whistle-blower and gives assurance that it will not reveal the identity of the Whistle-blower.

7.7.2 The only exception to this assurance relates to an overriding legal obligation to breach confidentiality. Thus, the Group is obligated to reveal confidential information relating to a Whistle blowing report, if ordered to do so by a court of law.

7.7.3 FirstCap Group's assurance of confidentiality can only be completely effective if the Whistle blower likewise maintains confidentiality.

## 7.8 **Confidential Information**

Confidential information is any item of information (verbal, written, or electronic) obtained in the course of an employee's employment, which is not in the public domain and is received with the reasonable expectation or a contractual agreement that the information will remain confidential.

## 7.9 **Designated Officer**

The head of Internal Audit/Head of Audit, who has been appointed or designated to manage Whistle blowers' cases confidentially by:

7.9.1 Receiving Concerns from and communicating with (potential) Whistle blowers;

7.9.2 Conducting a Preliminary Investigation; and

7.9.3 Providing information and reporting to relevant stakeholders, including the Board Audit Committee, on a strict "Need to Know" basis.

## 7.10 **Employees**

Employees of the Group in the context of this Policy shall include the following:

7.10.1 Permanent employees;

7.10.2 Independent consultants;

7.10.3 Interns;

7.10.4 Contractors and secondees;

7.10.5 Consultants (excluding consultants providing external assurance services); and

7.10.6 Any other category of staff, regardless of specific job responsibilities, department or location.

7.11 **FirstCap Group’s Designated Officer**

The Head of Internal Audit of FirstCap Limited.

7.12 **FirstCap Group**

The combination of:

7.12.1 FirstCap Limited; and

7.12.2 FBNQuest Funds Limited.

7.13 **Full Investigation**

The investigation following the Preliminary Investigation conducted in accordance with the Group’s Policy.

7.14 **Good Faith**

A Concern is reported in Good Faith when the Concern is not raised maliciously and when it is based on reasonable facts and/or circumstances that allow for the assumption that the Concern is sufficiently grounded.

7.15 **Investigation**

Preliminary Investigation and/or Full Investigation.

7.16 **“Need-to-Know” Principle**

This simply means that confidential information should only be communicated or disclosed to those who have legitimate need to have or be in possession of such information. In other words, information must not be communicated or transferred to anyone who does not have a legitimate need to be in the know. It also means that communication of Confidential Information shall not take place unless strictly required for the proper discharge of the employee’s

function and not contrary to the terms of any confidentiality agreement unless disclosure is required by law.

**7.17 Preliminary Investigation**

An inquiry to determine:

7.17.1 Whether the reported Concern is within the scope of this Policy; and, if so,

7.17.2 Whether there are reasonable facts and/or circumstances to start a Full Investigation in order to confirm or reject the Concern.

**7.18 Protected Disclosures**

Any statement or communications made pursuant to this Policy.

**7.19 Retaliation**

Retaliation is any adverse action taken against a Whistle-blower as a result of reporting the Concern or taken against any other employee who provides information, who causes information to be provided, or who otherwise assists in an Investigation. Examples of such adverse actions could include, but not limited to, harassing, threatening, firing or demotion, reducing benefits, transferring to another part of the Group, changing office location or changing responsibilities.

**7.20 Whistle blowing**

The reporting of Concerns relating to alleged unethical conduct by employees, directors, clients, service providers, vendors, creditors and other FirstCap Group's stakeholders by an employee or other persons to the Group, the SEC, or any other appropriate authorities.

7.21

**Whistle blower**

A Whistle blower is any person(s), including employees, directors, clients, service providers, vendors, creditors and other stakeholders who report Concerns to the Group, the SEC or any other appropriate authorities.

RENEWAL

**Contact Person:**

Name: **Segun Ilesanmi**

Title: Head, Risk Management & Compliance

Department: Risk Management & Compliance

Telephone: +234 (1) 279 8300 (ext. 2623)

Email: [segun.ilesanmi@firstcapltd.com](mailto:segun.ilesanmi@firstcapltd.com)

Key Words: Alternative Channel  
Anonymity  
Confidentiality  
Deviation  
Hotline  
Retaliation  
Waiver  
Whistle blower  
Whistle blowing  
Whistle blowing Policy



The FirstCap Group Designated Officer is:

Name: **Elizabeth Akinde**

Title: Head, Internal Audit

Department: Internal Audit

Telephone: +234 (1) 279 8300 (ext. 1248)

Email: [Elizabeth.Akinde@firstcapltd.com](mailto:Elizabeth.Akinde@firstcapltd.com)

Telephone (Internal): +234 (1) 279 8300 (ext. 1248)

E-mail (Internal): [whistleblowing@firstcapltd.com](mailto:whistleblowing@firstcapltd.com)

Telephone (External): 0817 597 8505

E-mail (External): [FBNHoldingsWhistleBlowing@first-holdco.com](mailto:FBNHoldingsWhistleBlowing@first-holdco.com)

The external telephone (“hotline”) is managed by the Head of Audit, First HoldCo Plc. The Head of Audit is not permitted to divulge the identity of the caller to FirstCap or its subsidiary (in the event the Head of Audit becomes aware of the caller’s identity).

## 11 Annexure C – The Reporting Process

- 11.1 An internal Whistle blower may raise a Concern either by disclosing his or her identity or anonymously through any of the following:
- 11.1.1 By calling the dedicated internal “hotline” (telephone number) under Annexure B;
  - 11.1.2 By calling or texting the external dedicated “hotline” (telephone number) under Annexure B;
  - 11.1.3 By sending e-mail(s) to the dedicated Whistle blowing e-mail address provided under Annexure B; and
  - 11.1.4 Directly raise Concerns to any of the relevant regulators.
- 11.2 An external Whistle blower may raise a Concern either by disclosing his or her identity or anonymously through any of the following:
- 11.2.1 By a formal letter addressed to the Head of Internal Audit and marked “Strictly Confidential;”
  - 11.2.2 By calling the dedicated hotlines as contained in the Group’s Whistle-blowing Policy hoisted on the Group’s Website, [www.firstcapltd.com](http://www.firstcapltd.com);
  - 11.2.3 By sending e-mail(s) to the dedicated Whistle blowing e-mail address as contained in the Group’s Whistle blowing Policy hoisted on the Group’s Website, [www.firstcapltd.com](http://www.firstcapltd.com);
- 11.3 The Designated Officer must, to the extent possible, acknowledge receipt of the Concern to the Whistle-blower.
- 11.4 The Designated Officer must, to the extent possible, inform the Whistle blower if the Concern is in scope of this Policy and, if so, his or her rights, obligations,

protections and next steps. This information specifically includes provisions regarding Confidentiality and Anonymity.

- 11.5 The Designated Officer must inform the Managing Director/CEO about the receipt of a Concern, without disclosing the identity of the Whistle blower. If the CEO is the subject of the Concern, the Chairman of the Board Audit and Risk Committee must be informed.
- 11.6 On a regular basis, the Whistle blower may request the Designated Officer to provide him or her with an update or feedback by providing a general status report on the progress of the investigation, but not on the details of the investigation itself. The Dedicated Officer can decide to refrain from providing an update on or certain details of the Investigation, for example, if he or she believes that such information is Confidential or could hinder the Investigation.
- 11.7 If the Concern affects the Designated Officer or the Whistle blower is uncomfortable or unable to raise the Concern through the Group's internal hotline or e-mail, the Whistle-blower is encouraged to raise his or her Concern through the external hotline.
- 11.8 As a last resort, the Whistle blower may consider raising his or her Concern to any of the relevant regulators.
- 11.9 Please note that during the conversation through the hotline (internal or external); the operator will request as much information as possible to ensure that the Investigator has sufficient information to commence an investigation. For the external hotline, the Head of Audit, First HoldCo Plc responsible for managing the hotline will submit a report to the Designated Officer of the Group to enable him or her action such reports.

## 12.1 Preliminary Investigation Process

12.1.1 If the reported Concern falls within the scope of this Policy, the Designated Officer must perform a Preliminary Investigation. Cooperation of employees, including senior management employees, is mandatory.

12.1.2 The Preliminary Investigation must in principle be concluded within one month of the receipt of the Reported Concern.

12.1.3 The Designated Officer may consult with other relevant stakeholders to determine if there are reasonable facts and/or circumstances from the Preliminary Investigation to conclude that the reported Concern is sufficiently grounded.

12.1.4 The Designated Officer must consult with relevant stakeholders, including the Managing Director/CEO or the Chairman of the Board Audit and Risk Committee, if the Preliminary Investigation indicates that (a member of) senior management is the subject of the Concern.

## 12.2 Full Investigation

12.2.1 If there are reasonable facts and/or circumstances resulting from the Preliminary Investigation that the reported Concern is sufficiently grounded, the Designated Officer will carry out a Full Investigation.

12.2.2 The Full Investigation and the case settlement will be carried out according to the Group's Policy. Cooperation by employees and directors is mandatory.

12.2.3 Where it is established that a criminal act has taken place, the matter may be referred to a law enforcement agency such as the Police, and where necessary, appropriate legal action taken.

12.2.4 Upon conclusion of the Investigation, the Designated Officer shall document his or her findings and recommendations and circulate same in line with the Group's Policy. In addition, the Designated Officer shall report to the Board Audit and Risk Committee (BARC), on a quarterly basis, the summary of cases reported, and the result of the investigations conducted on those cases.

RENEWAL

## APPROVAL PAGE

THIS COMPLIANCE POLICY WAS REVIEWED BY THE BOARD AUDIT AND RISK COMMITTEE  
AND RECOMMENDED FOR THE APPROVAL OF THE BOARD OF DIRECTORS

TODAY THE

---

CHAIRMAN, BOARD AUDIT AND RISK COMMITTEE

REVIEWED AND APPROVED BY THE BOARD OF DIRECTORS OF FIRSTCAP LIMITED.

TODAY THE

---

CHAIRMAN, BOARD OF DIRECTORS