



WHISTLEBLOWER POLICY

Version Number	Creation/ Revision Date	Prepared /Updated By	Reviewed By	Approved By	Change Description
1.0	01.06.2021	Compliance & Risk Committee	RiskPro	Group CEO	No Changes
1.1	17.11.2021	Compliance & Risk Committee	RiskPro	Group CEO	Removed Ombudsman references, removed hotline and updated related document list
1.2	18.05.2022	Compliance & Risk Committee	RiskPro	Group CEO	Added the acronyms table; Updated 1.1 Section. Added references related to Hotline and Suggestion boxes in section 2.8.2 and 2.8.3, updated the references accordingly in other sections.

TECHNO BRAIN WHISTLEBLOWER POLICY

INTRODUCTION

1.1 Background

The Whistleblower Policy (“the Policy”) is a supplement to the Code of Conduct and Ethics Policy (“the Code”) which describes the behaviors we expect Employees to demonstrate as representatives and ambassadors of our Company. The Company’s reputation for honesty and integrity is reflected in the way it conducts business, including in the integrity of its financial reporting.

Techno Brain and its subsidiaries (“the Company”) cultivate a culture where Employees can report, without fear of retaliation, any wrongdoing or misconduct which they suspect or believe may be occurring at the Company. Even if Employees only suspect alleged wrongdoing or misconduct, they are obligated to report it immediately. By doing so, they help the Company manage its reputational risk and any personal risk to themselves.

The Policy guides Employees through all aspects of the Whistleblower program including the reporting of suspected or actual, unlawful or inappropriate misconduct relating to material financial accounting, internal accounting controls, auditing matters, compliance requirements, and breaches of the Code of conduct.

This Policy is provided to all Employees upon hire and is also available on the Company’s intranet and the Techno Brain external website. Employees are required to review and attest to their understanding of this Policy annually as part of periodic attestation of the Code of Conduct.

It is also important to note that the Techno Brain Group Code is applicable to all entities of Techno Brain Group and to all employees. Further all employees must sign a declaration form annually acknowledging that the whistleblowing policy is conditional to their employment and that they have read, understood the policies and commit to abide by it. ICP policies must be signed by all staff at the time of commencement of employment and annually thereafter.

1.2 Purpose

The Whistleblower Policy is designed to provide assurance that business misconduct or other wrongdoing is reported, and that employees and external parties have a confidential channel to raise concerns for review and investigation. The Policy also protects the whistleblower from retaliation for disclosures made in good faith.

1.3 Scope

This Policy is applicable to entities of Techno Brain Group and to all employees of the Company.

2.0 Policy Requirements

2.1 Types of Concerns

2.1.1 Financial Reporting

Financial accounting, internal accounting controls and auditing matters, including those involving the circumvention or attempted circumvention of internal accounting controls or that would otherwise constitute a violation of Techno Brain's accounting policies. Examples include: falsification or destruction of business or financial records; misrepresentation or suppression of financial information; non-adherence to internal financial policies or controls; and auditor independence concerns.

2.1.2 Suspected Fraudulent Activity

Examples include: theft; defalcation; and corrupt practices including giving or receiving bribes or other unlawful or improper payments or benefits or falsification of records.

2.1.3 Breaches of the Code of Conduct and other compliance requirements

Any potential Breaches of the Code of Conduct, Compliance Requirements and other internal controls. Examples include: insider trading; conflicts of interest; short selling; market manipulation; non-adherence to internal compliance policies; illegal, deceptive or anti-competitive sales practices; and manipulation of rates.

2.1.4 Retaliation or retribution against an individual who reports a concern

Retaliation against employees who allege misconduct related to the above allegations. Examples include: statements, conduct or actions involving terminating, suspending, demoting; disciplining, suspending, harassing, intimidating, coercing or discriminating against an employee reporting a concern in good faith in accordance with this Policy.

2.2 Obligation to report concerns

All employees have an obligation to report real or perceived concerns. Employees are required to report concerns as soon as they become aware of the situation that raises the concern, with as many facts and as much detailed information as possible. The Company has a process to encourage employees to report concerns that contravene or are thought to contravene its Code of Conduct and Ethics Policy or situations where wrongdoing is suspected and employees are encouraged to use such processes.

If an allegation is made in good faith, but it is not validated through a review, no disciplinary action will be taken against the employee reporting the concern. If, however, an allegation is made frivolously, maliciously or for personal gain, disciplinary action may be taken against the employee. Intentionally or recklessly accusing an individual of wrongdoing, which the employee knows, or reasonably ought to know, is false, is a serious matter and is subject to disciplinary action.

2.3 Anonymous Reports

This Policy encourages employees to come forward in person wherever possible. Concerns expressed anonymously are much less powerful but will be considered based on a number of factors including the seriousness of the issues raised, the credibility of the concern, and the likelihood of confirming the allegation through credible sources and/or documentary evidence.

2.4 Acknowledgement of Report

Every reported incident will be acknowledged within twenty-four hours of receipt (factoring in weekends and public holidays) with the exception of anonymous reports.

2.5 Review & Investigation of Concerns

The Company will commence a review/investigation of all received concerns, regardless of the channel in which it was received. All concerns received will be documented and tracked until such time as the investigation is closed.

At a minimum, the reporting employee will be advised of the status of the review/investigation, that the review/investigation has been concluded and, where possible, the steps that were taken to resolve or prevent future occurrences, while respecting the privacy of all those involved.

2.5.1 Investigation steps include the following:

- Step 1: The committee members notified of the situation through speak up channels
- Step 2: Gather and review information
- Step 3: On a needs basis an expert might be engaged to provide intelligence into the subject matter under investigation
- Step 4: Structuring of the investigation wherein the CRC members/panel shall be assigned scope of investigation, terms and objectives are drawn.
- Step 5 Interview of the witnesses which can include internal and external as advised by the Compliance & Risk Committee
- Step 6: Preparation of investigation report
- Step 7: HR to schedule a disciplinary hearing based on the evidence collected
- Step 8: Corrective actions to be enforced as per TBG's disciplinary policy

Any investigation outcome must be summarized in a report with clearly documented evidence and corrective measures enforced.

2.6 Confidentiality

Unless compelled by judicial or other legal process to reveal the identity of the employee who makes an allegation under this Policy, the individual will remain confidential. No effort to ascertain the identity of any person or group who makes a report anonymously will be tolerated.

2.7 Protection from Retaliation

The Company shall not tolerate any retaliation by management or any other person or group, directly or indirectly, against anyone who in good faith makes an allegation or report under this Policy, and who provides assistance to management or any other person or group, including any governmental, regulatory or law enforcement body, investigating a report. Anyone who retaliates in any way against a person who has made a good faith allegation will be subject to disciplinary action.

2.8 Methods for Reporting Concerns

Employees can use any of the following methods to report a concern.

2.8.1 Code of Conduct and Whistleblower email

The reporting channel is through; email: tbgethics@technobraingroup.com

Intended for the reporting of suggestions and concerns related to:

- Code of Business Conduct and Ethics
- Privacy
- Internal Fraud
- Finance and Accounting
- Discrimination and Harassment

- Employees using this method will not receive follow-up on their concerns if they choose to remain anonymous.

Individuals outside of the organization can also raise a concern through the Whistleblower email provided above.

2.8.2 Suggestion box

Suggestion box is one of the reporting channels in Techno Brain's physical offices available to all employees and contractors. This channel is used as an alternate method for collecting all kind of feedback on a day to day basis. We communicate to employees about the usage of suggestion box through monthly "Open House" meetings, onboarding programs, HR connects, including walk-ins from our field employees. Suggestion boxes are placed in each country office in a private corridor. The feedback from suggestion box is collected by HR on fortnight basis and compliance related concerns are shared with CO/CRC committee for further investigation and action as required.

2.8.3. Whistleblower hotline

Additionally, this is a reporting channels through direct call dialing to Techno Brain's physical offices available to all interacting parties from Kenya and Uganda of Techno Brain. The hotline number 0800721568 (Kenya – Toll free number) and +254709581999 (Any other locations), which is publicly published on the Company's website. This channel is used as an alternate method for collecting all kind of feedback on a day-to-day basis. We communicate to employees about the usage of whistleblower hotline through monthly "Open House" meetings, onboarding programs, HR connects, mailers/in-house flyers, notice boards and/or word of mouth through the HR office in all our country offices.

The feedback from the hotline is collected by HR on a daily basis and compliance related concerns are shared with CO/CRC committee for further investigation and action as required through an ICP reporting issue tracker.

2.8.4 Contact Human Resources

Employees may contact the SBU Head, Human Resources to report their concern. Human Resources will review and escalate any concerns, as well as protect the reputation of the company.

2.8.5 Contact Chair of Committee and Risk Committee

If an Employee is not comfortable raising their concern through one of the options above, or their concern specifically relates to the following parties:

- Head of Human Resources (HR Business Partner)
- Compliance Officer (CO)
- Group Chief Executive Officer (CEO)
- Board of Directors

3.0 Roles and Responsibilities

3.1 Introduction

This section sets out the responsibilities for Employees, People Leaders, Senior Management, Human Resources and the Board to support the Whistleblower Policy, but it is not meant to be exhaustive.

3.2 Employees

Employees are expected to:

- Ensure their understanding and compliance with the Whistleblower Policy, Code of Conduct & Ethics and any policies, guidelines and procedures that support the Whistleblower Policy;
- Identify and immediately report any suspected or known Wrongdoing;
- Complete annual training and attestation with respect to the Whistleblower Policy, Code of Conduct & Ethics and any supporting policies

3.3 People Leaders and Senior Management

People Leaders and Senior Management are expected to:

- Ensure that all direct reports understand and comply with the Code of Conduct;
- Ensure that all annual training (and attestations) is completed in the timeframe required;
- Encourage an environment of open communication and high ethical standards;
- Be familiar with the laws and regulatory requirements that apply to the Company and relevant business processes.

3.4 SBU Head, HR, CO, and Director, Legal and Corporate Secretary

These executives are expected to:

- Commence a review/investigation of all concerns received, regardless of the channel in which it was received (the CO is responsible for independently reviewing/investigating all concerns received that relate to HR team members);
- Document, track, investigate and report on concerns reported, ensuring that as much information as possible is gathered to fully investigate the concern raised;
- Document, track, investigate and report concerns regarding Code of Conduct breaches.
- Engage subject matter experts as required to satisfactorily investigate the concern raised;
- Provide timely notification to the Chair of the Compliance and Risk Committee of all Whistleblower complaints;
- Track all concerns raised and report to the Board of Directors quarterly, or on an as-needed basis;
- Ensure the approved Whistleblower Policy is immediately posted by Human Resources on the Techno Brain website and internal website following approval from the Board.

3.5 Chair of the Compliance and Risk Committee and the Board of Directors

The Board of Directors has ultimate responsibility for this Policy. The Board of Directors has delegated its responsibilities to the Compliance and Risk Committee.

The Chair of the Compliance and Risk Committee is responsible for:

- Ensuring that any Whistleblower Policy reporting is received and reviewed;
- Ensuring that proper reviews/investigations are completed, and that appropriate corrective action is taken;
- Ensuring that any concerns received regarding the CEO, SBU Head, HR and CO are immediately communicated to the Chair of the Board;
- Ensuring that the appropriate parties are engaged to complete the review/investigation of any concerns raised regarding the CEO, SBU Head, HR and CO.
- Expected to direct any external concerns received that fall under this Policy to the CEO, Human Resources, the SBU Head, Compliance Officer, or the Chair of the Compliance and Risk Committee

Once every two years, each Board member must review the Whistleblower Policy and attest to their compliance with the Policy on a regular basis.

4.0 Monitoring and Reporting

4.1 Policy Monitoring

The completion of training and attestations related to the Whistleblower Policy are monitored by Human Resources.

4.2 Policy Reporting

4.2.1 Reporting Internal Concerns

Internal concerns reported through the Whistleblower program are reported according to the following table

Involved Parties	Reported by	Reported to
Any parties except HR team members, President & CEO or CO	SBU Head, Human Resources	Chair of Compliance and Risk Committee
Member of HR team	CO	Chair of Compliance and Risk Committee
Chief Executive Officer, SBU Head, HR or CO	Chair of Compliance and Risk Committee	Chair of the Board

4.2.2 External Reports

If a concern comes from an external source through the CRC and the General Counsel and Corporate Secretary, the concern will be directed to the SBU Head, Human Resources, Compliance Officer, or the Chair of Compliance and Risk Committee.

5.0 Review and Approval

The Whistleblower Policy is subject to review once every two years or when business needs arises and subsequently all employees shall be updated of the changes.

The Compliance and Risk Committee reviews and recommends the Policy for approval to the Board of Directors.

There are no exceptions granted for this policy.

Non-compliance with the Policy should be reported to the SBU Head, HR immediately for remedial action.

6.0 Relevant Regulatory Requirements

Relevant legislative and regulatory requirements include the Country specific Criminal Code, Whistleblower program and other relevant Act. These provisions are intended to ensure that appropriate mechanisms are in place to protect Employees from any form of whistleblower reprisal.

7.0 Effective Date

Compliance with this Policy is to take effect immediately following approval by the Board of Directors.

8.0 Related Documents

This Policy should be read in relation to the following documents:

- ISPMS-PO-Acceptable-Usage Policy
- Antitrust & Antifraud policy
- Code of Conduct
- Human Rights, Equal Opportunity and Harassment guidelines provided in the employee handbook and Recruitment & Selection policy and Workplace Violence policy.
- Techno Brain Group-ISPMS Manual
- Reporting a Whistleblower Concern through an email tbgethics@technobraingroup.com

9.0 Confidentiality

This policy is available to the public through the Techno Brain website.

10.0 Acronyms

CEO	Chief Executive Officer
CRC	Compliance and Risk Committee
CO	Compliance Officer
SBU	Strategic Business Unit
HR	Human Resource
ISPMS	Information Security and Privacy Management System