TECHNO BRAIN

Empowering Lives

HOTLINE-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

TECHNO BRAIN HOTLINE-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.

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.

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 applies to all Employees (as defined in section 2. Definitions) of the Company.

2.0 Definitions

Breach - is defined as non-compliance with an applicable law, regulation, internal policy or procedure.

Employees – refers to the Company's directors, full-time Employees, part-time Employees, temporary Employees and contractors employed by Techno Brain and any of its subsidiaries.

Compliance Requirements - Refers to an applicable law undertaking to legislative authority or provision, section, subsection, order, term, condition and procedure that requires the Company to do (or prohibits the Company from doing) certain things or to act or conduct its affairs in a particular manner.

People Leaders – are defined as anyone who has Employees reporting to them.

Policies – in this Policy, includes company guidelines, procedures and practices.

Retaliation – an action having a negative impact or implication against an individual who has reported a concern.

Wrongdoing – the act of doing something illegally or dishonestly or that is a Breach.

Senior Management – is defined as anyone holding a position titled Director and above

3.0 Risk Appetite

Risk Appetite: Key Principles	
1. We maintain adequate capital and liquidity at all times. 2. We only take risks that are transparent, manageable and fit our business strategy. 3. We do not expose the Company to any significant single loss events on any individual transaction or acquisition. 4. We do not take risks that are expected to result in significant volatility in earnings or shareholder returns. 5. We conduct business with honesty, integrity, respect and high ethical standards. 6. We strive to protect the Company's reputation at all times, with all key stakeholders.	7. We adopt a risk based approach for identifying, assessing, managing, mitigating and monitoring risk that meets regulatory requirements and expectations. 8. We do not tolerate business activities that are not supported by appropriate processes and internal controls that are designed to detect, deter and prevent activity associated with financial crime. We do not maintain relationships with persons or entities believed to be engaged in illegal or illicit activities. 9. We incorporate risk and compliance measures into performance and reward measurement programs.

4.0 Policy Requirements

4.1 Types of Concerns

4.1.1 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.

4.1.2 Suspected Fraudulent Activity

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

4.1.3 Breaches of the code 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.

4.1.4 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.

4.2 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 wrong doing 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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

4.7 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.

4.8 Methods for Reporting Concerns

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

4.8.1 Code of Conduct and Whistleblower Hotline

The hotline channel; Internal email: speakup@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 Hotline.

4.8.2 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.

4.8.3 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:

- Group Chief Executive Officer (CEO),
- Head of Human Resources (HR Lead)
- Compliance Officer (CO)

5.0 ROLES AND RESPONSIBILITIES

5.1 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.

5.2 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

5.3 People Leaders and Senior Management

People Leaders and Senior Management are expected to:

- Ensure that all direct reports understand and comply with the Code;
- Ensure that all annual training (and attestations) are 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.

5.4 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 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 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.

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

The Board of Directors has ultimate responsibility for the 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.

On an annual basis, every Board member must review the Whistleblower Policy and attest their compliance with the Policy.

5.6 Ombudsman

The Ombudsman is 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.

6.0 Monitoring and Reporting

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

6.2 Policy Reporting

6.2.1 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

6.2.2 External Reports
If a concern comes from an external source through the Ombudsman 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.

7.0 Review and Approval

The Whistleblower Policy is subject to review at least on a biennial basis.

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. Significant instances of non-compliance are reported to the Chair of Compliance and Risk Committee.

8.0 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.

9.0 Effective Date

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

10.0 Related Documents

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

- Acceptable Use Policy
- Anti-Fraud Policy
- Code of Conduct and Ethics Policy
- Human Rights, Equal Opportunity and Harassment Policy
- Information Security Policy
- Records Management Policy
- Reporting a Whistleblower Concern Document

11.0 Confidentiality

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