INDIA POLICIES DOCUMENT

Whistle blower Policy

Policy Level: Regional-India
Approval Authority: Equifax Credit Information Service Pvt Ltd (ECIS) Board
Policy Owner: Shreenivasrao D Dandapati, Chief Compliance & Data Protection Officer
Policy Administrator: Arijit Sen, Compliance Officer
Effective Date : June 2, 2025
Last Approved: June 10, 2025
Next Review: 24 Months from the Last date of Approval

OVERVIEW

It is important to ECIS that any fraud, misconduct, bribery or other wrongdoing is reported and properly dealt with. It is the responsibility of all Employees to raise any concerns they might have about malpractice within the workplace. ECIS therefore encourages all Employees to raise any concerns they may have about the conduct of others in the business or the way in which the business is run. This is in accordance with the company's values (e.g. Do The Right Thing, Customer First), and the Boards Risk Appetite, whilst maintaining compliance with all applicable laws, regulations and industry standards and delivering good outcomes for Consumers.

This Policy applies to all Full time and Contractual employees of the Company,

This document should be read in conjunction with the Code of Ethics and Business Conduct Policy

Contents

1. STATEMENT OF OBJECTIVES

It is ECIS policy to conduct all business in an honest and ethical manner. The company has no appetite for regulatory breach, fine or censure and therefore supports Employees' rights to raise concerns. The company is committed to acting professionally, fairly and with integrity in all its business dealings and relationships wherever it operates.

This Policy sets the key requirements to meet the company's expectations regarding whistleblowing. The process by which Employees and other stakeholders may raise their concerns, and how the company will deal with those concerns are set out in the Appendix A

In relation to conduct and raising concerns, the Company's Risk Appetite states:

- *We have no tolerance for intentional breaches of regulatory requirements, including (without limitation) any laws, regulations, standards, principles, rules, directions, conduct requirements or guidance, or of our policies and standards.*
- *All known deviations from regulatory requirements or our policies and standards must be reviewed and escalated as appropriate and as a time bound policy exception or risk tolerance; any breaches must be remediated in line with prescribed timescales. Any breaches that meet regulatory notification requirements will be escalated and reported to the relevant authorities or regulators, as required.*
- *We promote and require high standards of conduct and compliance without exception with regard to integrity from our employees. All employees are expected to act with the highest standards of integrity and in line with our legal and regulatory obligations, understanding the impact of their decisions and behaviours on customer outcomes. Our actions will aim to place our customers at the centre of everything we do and we will be open and transparent in all of our dealings. Actions that could cause our integrity to be challenged will be subjected to appropriate scrutiny.*

2. PRIMARY REQUIREMENTS

2.1. The company will encourage Employees to raise their concerns under the procedure outlined in **Appendix A** of this Policy in the first instance. Employees can be comfortable in bringing forward

their concerns in the secure knowledge that they will be taken seriously, anonymously if they wish and with no adverse repercussions where the Employee has acted in good faith. The Company aims to acknowledge receipt of a whistleblowing report within 7 days.

2.2. Employees should be aware of the importance of eliminating fraud, misconduct, bribery, conflicts of interest or other wrongdoing at work. They should report anything they become aware of that falls within the definitions contained in Section 7. Reports of personal grievances, harassment and bullying are generally not covered under whistleblowing. Matters of this nature should be raised with your manager and/or HR.

2.3. All Qualifying Disclosure will be taken seriously. The disclosure will be promptly and fairly investigated by a designated investigator (Chief Compliance Officer or General Counsel or Senior HR Business Partner or one of their nominated delegates.) If, upon conclusion of the investigation, the individual reasonably believes that appropriate action has still not been taken, they may then report the matter to any authority as they may deem appropriate.

2.4. As part of the investigatory process, the Employee may be interviewed and asked to provide a written witness statement setting out the nature and details of the disclosure and the basis for it. Where the whistleblower has elected to remain anonymous this may not be required or arrangements will be put in place to obtain the information without exposing the individual's identity.

2.5. The Whistleblower has to directly raise the issues / report the suspected instance through writing an email to the Chief Compliance Officer.

2.6. It will not be necessary for an Employee to have proof that an act is being, has been, or is likely to be committed – a reasonable belief is sufficient, even if that belief later turns out to be wrong.

2.7. The company will take responsibility for ensuring an appropriate investigation takes place. Employees have no responsibility for investigating a matter they have raised concerns about.

2.8. Employees will not be victimised, subjected to detriment or dismissed for raising a genuinely- held concern in good faith under this Policy, even if their disclosure is not upheld. There is no qualifying period of employment for this protection.

2.9. A disclosure made maliciously, in bad faith or with a view to personal gain, may lead to the Whistleblower being subject to disciplinary action.

2.10. Employees who victimise or retaliate against those who have raised concerns under this Policy will be subject to disciplinary action, up to and including dismissal/termination of employment.

2.11. Covering up someone else's wrongdoing is a disciplinary offence. Employees should never agree to remain silent about wrongdoing, even if told to do so by a person in authority.

2.12. A Qualifying Disclosure or Relevant Wrongdoing is protected if it is made under the terms of this Policy and the Procedures contained in this document. Employees must act in the public interest at all times.

2.13. The company will review and implement any recommendations for change to minimise the risk of a

recurrence of any malpractice or impropriety which has been uncovered. If no action is to be taken, the reasons for this will, as appropriate, be explained to the Whistleblower.

2.14. Appropriate management information will be produced to inform the Board and senior managers of issues arising, with due regard to confidentiality where necessary.

3. MONITORING AND TESTING

The Policy Owner is responsible for monitoring adherence to this policy. This is ensured via training provided at onboarding and annually, and regular oversight reviews.

Second Line of Defence functions may conduct testing to confirm adherence to and sufficiency of Policies; the frequency of such testing is risk-based.

The Third Line of Defence, will assess the adequacy of adherence to policies and standards during planned internal audit activity. Internal Audit activities are planned and performed using a risk based approach.

4. TRAINING AND COMMUNICATION

It is the company's goal to provide all Employees with a basic understanding of this Policy. Mandatory training is provided at onboarding and on an annual basis. However, certain employees are more likely to confront issues based on their job function. In an effort to ensure that such employees have an understanding of the ways in which Whistleblowing will affect their specific business responsibilities, the Company may require that certain employees attend targeted training sessions.

5. ADMINISTRATION AND GOVERNANCE

Compliance with this Policy is a condition of continued employment or continued business relationship with the company. Violation of this Policy will be considered a breach of trust and may result in internal disciplinary action, up to and including termination.

There are no exceptions to this policy. Any exceptions to or violations of the Policy must be reported to the Policy Owner, via the Indiacompliance@equifax.com mailbox, or in accordance with the Whistleblowing procedure set out in this Policy.

At least once every two years or when material internal or external changes occur, the Policy Owner will review and, if necessary, submit appropriate changes to this Policy for approval. The review may include, amongst other things, consideration of regulatory guidelines, BU feedback on the effectiveness of the Policy, and any supervisory or audit input.

Minor changes such as typographical corrections, formatting, Policy ownership and/or immaterial changes to a Company Policy do not require a formal vetting process but may be made under the Policy Owner's discretion. An immaterial change is defined as one that will not alter the process or primary requirements of the Policy but alternatively provides clarity in the process or roles and responsibilities.

Interested parties should forward questions or suggestions about this Policy to the Policy Administrator or Owner.

6. ROLES AND RESPONSIBILITIES

Role	Responsibility
ECIS Board of Directors	Provide leadership and oversight of all business activity. The Board will: • Ensure that Operational Management understands its obligations in relation to Whistleblowing. • Receive regular reports on risks and issues that may indicate exposure to fraud, misconduct, bribery, conflicts of interest or other wrongdoing at work. • Take or direct appropriate action to define and implement remedial activity to mitigate risks related to fraud, misconduct, bribery, conflicts of interest or other wrongdoing at work that have been identified. • Review and approve this Policy at least once every two years or when material internal or external changes occur. • Receive reports on adherence and monitor relevant resourcing to determine if it is sufficient to manage risk within appetite.
HR	• Provide training for all Employees at induction and for annual refresher. • Receive and deal with reports of inappropriate activity that may be submitted from time to time by Whistleblowers,
Legal department	• Receive and deal with reports of inappropriate activity that may be submitted from time to time by Whistleblowers,
Privacy & Compliance	• Receive and deal with reports of inappropriate activity that may be submitted from time to time by Whistleblowers. • Provide second line oversight and challenge on adherence to Compliance requirements and report to the Board about related Risk exposure. • Liaise with the RBI on regulatory compliance as necessary.
All Employees	• Read, acknowledge and comply with this Policy. • Report policy violations, problems and concerns to management in a timely manner. • Seek clarification from management concerning any questions or concerns with respect to compliance with the Policy. • Complete training as directed by management.

Policy Owner	• Ensure the Policy is reviewed at a frequency as defined in the policy. • Periodically review to confirm this document is not inconsistent or less restrictive than relevant documents. • Create and implement strategies for the communication and awareness of the Policy. • Interpret the requirements as necessary to support implementation by senior management. • Maintain a written record of exceptions approved, including the reasons for granting them. • Monitor adherence to the requirements in this Policy and the relevance of the Policy to the needs of the company. • Report inappropriate activity to the Board or appropriate sub-committees. • Be the contact person for enquiries relating to the content of the Policy. • Delegate responsibility to nominated deputies as appropriate whilst retaining accountability.

7. DEFINITIONS

Board: The Statutory Board(s) of the Equifax Credit Information Services Pvt Ltd (ECIS)

Company: Equifax Credit Information Services Pvt Ltd.

Consumer: Clients interacting with ECIS to view, purchase or discuss credit information of their customer..

Customer: An individual person ("D2C Customer")

First Line of Defence (1LOD): The First Line, i.e. Business Units (BUs), owns and manages risks and is responsible for: identifying, assessing, mitigating and communicating risks and maintaining effective internal controls.

Second Line of Defence (2LOD): The Second Line (e.g. Privacy & Compliance) provides credible challenge and oversight through measurement, monitoring and reporting of First Line business risk.

Third Line of Defence (3LOD): The Third Line (Internal Audit) provides independent and objective assurance to senior management that the First and Second Lines are functioning as intended & reporting on identified issues to the agreed BU governance.

Employee: An employee of the company, including those employed on fixed term, or contractual.

NDA: Non-disclosure agreement.

Qualifying Disclosure: Disclosure made in the public interest by an employee who has a reasonable belief that:

- A criminal offence has been committed, is being committed, or is likely to be committed;
- A person has failed, is failing, or is likely to fail to comply with a legal obligation;

- A miscarriage of justice has occurred, is occurring, or is likely to occur;
- The health and safety of any individual has been, is being or is likely to be endangered; or
- The physical environment has been, is being or is likely to be damaged..

Whistleblower: A person who exposes information or activity that is deemed illegal, dishonest or not correct within an organisation that is either private or public.

Policy Owner: The individual or entity responsible for creating, implementing, and ensuring compliance with a specific policy within the organization.

8. REFERENCES

Equifax Global Code of Conduct
Whistleblowing Process Guide
The Whistleblower Protection Act, 2011
The Companies Act, 2013

9. REVISION HISTORY

As part of the overall document control process all updates, approvals and version reviews are documented in the following sections.

Version	Description	Edited by	Reviewed By	Date
1.0	First Draft	Arijit Sen	Shreenivasrao D. Dandapati	May 31, 2025

APPENDIX A – Whistleblowing / disclosure procedure

This procedure applies to all full time and contractual employees. In addition, third parties such as agency workers, consultants and contractors and any others who perform functions in relation to the ECIS are encouraged to use it.

In the event of an individual wishing to make a qualifying disclosure, they should follow the steps below:

- Report it by writing, email to whistleblowerindia@equifax.com

OR

- via the Equifax Reporting Line (see below)

Equifax Integrity Line:

Country	Toll Free
India	**022-50972521**

OR

- Report the situation to their direct manager or the next level of management;

OR

- Report it to the Human Resources Department or a member of the Privacy & Compliance Team, or the Legal Team. The relevant Departmental Heads may also be emailed directly if preferred.

Disclosures should be made promptly so that an investigation may proceed and any action taken expeditiously.

Confidentiality will be maintained during the investigatory process to the extent that this is practical and appropriate in the circumstances. However, in order to effectively investigate a disclosure, the Company must be able to determine the scope of the investigation and the individuals who should be informed of or interviewed about the disclosure. If it becomes necessary to disclose the Whistleblower's identity, the company will make efforts to inform the Whistleblower that his or her identity is likely to be disclosed. In order not to jeopardise the investigation, the Whistleblower is also expected to keep the fact that they have raised a concern, the nature of the concern and the identity of those involved confidential.

The length and scope of the investigation will depend on the subject matter of the disclosure. The company reserves the right to arrange for another Manager to conduct the investigation other than the Manager with whom the individual raised the matter. In addition, an investigative team with experience of operating workplace procedures or specialist knowledge of the subject matter of the disclosure may be appointed. It is not normally appropriate to set a specific timeframe for completion of investigations in advance, because the diverse nature of disclosures makes this unworkable.

If initial enquiries by the Compliance Officer indicate that the concern has no basis, or it is not a matter to be investigated under this Policy, it may be dismissed at this stage and reason for dismissing the complaint, without further investigation, should be documented.

The investigation report along with disciplinary action as the Compliance Officer may think fit and preventive measures to avoid reoccurrence of the matter shall be prepared within 45 days from the receipt of the complaint, on a best effort basis. In case any extension in the timeline is required due to unforeseen reasons, the approval of the Audit committee will be obtained.

Once the investigation has been completed, the individual will be informed in writing of the outcome, together with the company's conclusions and decision in a timely manner. However, the need for confidentiality may prevent the Company from giving the employee specific details of the investigation or actions taken. The Company is committed to taking appropriate action with respect to all qualifying disclosures which are upheld. When the company's conclusions have been finalised, any necessary action will be taken. This could include either reporting the matter to an appropriate external Government Department or Regulatory Agency and/or taking internal disciplinary action against relevant employees. The Company will endeavour to inform the individual if a referral to an external agency is about to or has taken place, although it may be necessary to make such a referral without the individual's knowledge or consent if this is appropriate in the circumstances.

Depending upon the seriousness of the matter, the Compliance Officer may intimate the Audit Committee within 45 days from the date of the complaint with proposed disciplinary action/ counter measures for necessary action. The Audit Committee may decide the matter as it deems fit within the next 45 days. The decision of the Audit Committee would be final and binding.

In the event the complaint is against the Chairperson of the Audit Committee or the Chairperson discloses any conflict w.r.t complaint received, he/she shall recuse from the proceedings and the role of the Chairperson shall be carried out by one of the members selected by the remaining members of the Audit Committee.

If, upon conclusion of the above stages, the individual reasonably believes that appropriate action has still not been taken, they may then report the matter to the appropriate external authority in good faith.