GLOBAL ANTI-FRAUD POLICY

Master List Ref	Release Date	Review Date	Next Review Date
ERM – 01	January 6, 2014	February 05, 2026	January 31, 2027
Version: **1.1**	**Process Owner** Risk Management (I-ARM team)	**Reviewed by** SVP – Internal Audit and Risk Management	**Approved by** **Risk Management Committee**

This document is the sole property of Firstsource Solutions Limited. Any use or duplication of this document without express permission of Firstsource Solutions Limited is strictly forbidden and illegal.

Contents

1.	PURPOSE & OBJECTIVE	2
2	SCOPE & APPLICABILITY	2
3	WHAT IS FRAUD?	3
	3.1 Definition	3
	3.2 Illustrations	3
4	FRAUD MITIGATION STRATEGY	4
4	FRAUD PREVENTION & CONTROL	5
6	REPORTING & REVIEWING PROTOCOLS	8
	6.1 Fraud Reporting	8
	6.2 Inquiry & Investigation	9
	6.3 Disciplinary Actions	9
	6.4 Safeguard	9
7	AWARE	10
8	REVIEW	10

1. PURPOSE & OBJECTIVE

The Global Anti-Fraud policy aims to protect the brand, reputation, and assets of the Company from loss or damage resulting from suspected incidents of fraud, in addition to safeguarding the confidentiality of client and customer data used for providing services to our clients.

The policy aims to achieve the following objectives:

- Promote zero tolerance to fraud.
- Strengthen the anti-fraud culture across the Company,
- spread awareness and educate employees on fraud risks faced by the Company.
- encourage all employees / associates of Firstsource to report cases of fraud; and
- Identify and address organization vulnerabilities through proactive and reactive measures.

2. SCOPE & APPLICABILITY

This policy applies to all employees (full time and part time), associates & employees of associates of Firstsource and any parties having a business relationship with Firstsource. For this policy, associates of Firstsource include vendors, consultants, business partners and contractors.

3. WHAT IS FRAUD?

3.1: Definition

The Oxford dictionary defines fraud as “wrongful or criminal deception intended to result in financial or personal gain”.

Fraud can also be defined as “a wilful act committed by an individual or entity, by deception, suppression, cheating or by any other fraudulent or illegal means, thereby causing wrongful gain(s) to self and other individuals and wrongful loss to others”

Global Anti-Fraud Policy defines fraud as “any illegal, dishonest, or irregular act done knowingly and wilfully, whether by words or by conduct, which may result in a financial or non-financial loss to the Company. It includes:

Fraud is intentional act to achieve illicit gain

- Use of deception with the intention of pursuing personal interests and causing loss to the proper interests of the Company.
- Illegitimate pursuit of Company interests in an appropriate =manner for personal gain; and
- Intentional distortion of financial statements or other records by persons internal or external to the Company
- which is carried out to conceal misappropriation of assets or for personal gains”

Fraud can be perpetrated by an insider or outsider (employee or associate)

An individual or a group of people can commit fraud through collusion

Specific Exclusions: Irregularities concerning employee’s moral, ethical or behavioural conduct should be resolved by departmental management and Human Resource department rather than Fraud Risk Management (FRM) team.

In case there is any question as to whether an action constitutes fraud, contact the FRM team for guidance.

3.2: Illustrations

Listed below are few illustrations that could be construed as fraud. If in doubt, contact the FRM team at fraudhelpline@firstsource.com

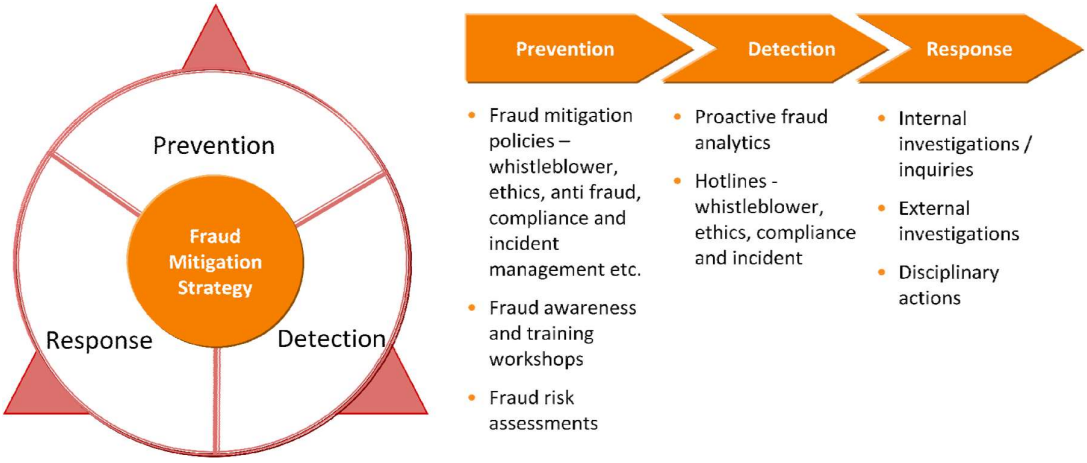
- Usurpation of corporate interests for personal gain.
- Misappropriation of assets, embezzlement, and theft.
- Payment or receipt of bribes, kickbacks, or other inappropriate payments.

- Deriving benefits for Company's interests through illicit or illegal means in collusion with external parties.
- Participation in sham or fraudulent transactions.
- Deceptive, misleading, or false statements about corporate transactions.
- Forgery or alteration of accounting record or vouchers.
- Unauthorized disclosure of trade secrets of the Company for personal gain.
- Non-disclosure of material information needed for an informed investment decision.
- Theft or misuse of confidential / sensitive information; and
- Other fraud behaviours' causing loss or illegal gain to the Company.

4. FRAUD MITIGATION STRATEGY

Fraud Mitigation Strategy at Firstsource focuses on fraud prevention, detection, and response ("Three Pillars" of Fraud Risk Management) to achieve the following objectives:

- Proactive identification and remediation of fraud risk.
- Educate and guide employees and strengthen fraud preparedness; and
- Timely fraud response through investigations, disciplinary actions, and process remediation



5. FRAUD PREVENTION & CONTROL

Prevention of fraud is everybody's responsibility. Management, employees, and associates of Firstsource are expected to be alert at all times and take necessary steps to report fraud.
The roles and responsibilities of all stakeholders are detailed below:

Stakeholder	Responsibility
Risk Committee	• Comprising of the Chief Executive Officer (CEO), Chief Financial Officer (CFO) and Chief Compliance Officer (CCO), it will provide guidance on the fraud mitigation strategy and related risks of Firstsource
Business & Function Heads	• Assess the risk of fraud arising in the normal business operations of each geography, process, and unit within their span. • Establish controls and procedures designed to eliminate the likelihood of occurrence of fraud. • Report and recommend a remedial course of action in respect to suspected or voiced concerns of fraud or fraudulent behavior. • Promote a regular corporate culture of honesty and integrity through the following actions and activities: o Lead by example in complying with the Global Anti-Fraud Policy. o Regularly communicate the Company's message of honesty and integrity with employees of the Company, through the Employee Handbook and other written and verbal presentations of the principles underlying in this Policy. o Conduct periodic meetings to ensure employees attend trainings regarding business ethics and the related laws and regulations. o Notify all direct or indirect interested parties, including external parties (customers, suppliers, supervision authorities and shareholders) regarding this Policy and the obligation of the employees to comply therewith. o Notify employees and external third parties of the opportunity and procedures for anonymously reporting wrongdoings and dishonest behavior; and o Identify and asses the importance and possibility of fraud risk at entity level, in each business department level and at all significant account's 7levels, in view of the Company's overall risk management assessment process.

Stakeholder	Responsibility
Fraud Risk Management (FRM) Team	• Design and develop the FRM framework. • Review, monitor, improve and implement security controls across the organization. • Assess and approve adequacy and appropriateness of security / fraud controls across all organizational functions covering operations, administration, facilities, physical security, human resources, technology, finance, sales & marketing and other support functions. • Assess, examine, and approve inter as well as intra departmental controls. • Sign off the policies, procedures and control designs for all departments covering the security / fraud prevention controls. • Access systems, policies, records, documents, SOPs, MIS, employees (team members) and any other information of all functions / departments across the Company, with the approval of any member of the Risk Committee, as an when the need arises. • Review and assess all reported cases of fraud. • Manage / conduct / coordinate all investigations and share reports with the designated personnel. • Recommend and follow through the disciplinary actions taken against the wrongdoers; and • Review and update, as necessary, the Global Anti-Fraud Policy on an annual basis.
Human Resources Team	• Obtain Declaration for reading, understanding, and agreeing to comply with the Global Anti-Fraud Policy from all employees. • Perform customary background checks (education, work experience and criminal records) for individuals being considered for employment or positions of trust; and • Formal written documents for background checks shall be retained and filed in employee's record.
All employees of the Company	• Ensure compliance with all FSL policies and procedures. • Report "all" cases of suspected fraud immediately on whistleblowing@firstsource.com ; • Do not tamper any evidence and do not try to investigate the case yourself. • Provide complete support and cooperation to the FRM team. • Act with the highest standards of ethics and integrity. • Acknowledge reading, understanding, and agreeing to comply with the Global Anti-Fraud Policy at the time of joining; and • Complete and pass the online Global Anti-Fraud Training on an annual basis.

Stakeholder	Responsibility
All associates of the Company	• Ensure compliance with all FSL policies and procedures. • Report "all" cases of suspected fraud immediately on whistleblowing@firstsource.com; • Do not tamper any evidence and do not try to investigate the case yourself. • Provide complete support and cooperation to the FRM team. • Act with the highest standards of ethics and integrity; and • Read, understand, and agree to comply with the Global Anti-Fraud Policy by signing the declaration of acceptance on an annual basis

6. REPORTING & REVIEWING PROTOCOLS

6.1: Fraud Reporting

At Firstsource, we foster an open communication culture. Any person (employee or associates of the Company) with knowledge of suspected incident of fraud or who is personally being coerced by others to participate in a fraudulent activity must report the case immediately.

All cases of suspected fraud can be reported to whistleblowing@firstsource.com and the Company shall strive to maintain any request for anonymity.

Carefully refer to the important aspects to be considered while reporting a suspected fraud incident.

Important: Do's

- **Report immediately / as soon as you are aware of an alleged incident Important: Do's**
- **Report immediately / as soon as you are aware of an alleged incident**
- **Provide the following information along with the incident:**
  - **Who is the suspect (name)**
  - **What has the suspect done**
  - **Copy of evidence that you may have**
  - **Other information like contact details,**
  - **program / process / department, names**
  - **of third parties, if any.**
  - **Your name and contact number, which**
  - **may be required to get further details if any**
- **Safeguard the original evidence**

Important: Don'ts

- **Do not delay in reporting the incident. The more you delay, the longer the exposure to the fraud which may mean greater losses to the Company and / or to you**
- **Do not hide any information while reporting the incident**
- **Do not tamper with any evidence / original documents**
- **Do not try to investigate the incident yourself**
- **Do not share information with anybody.**
- **Process as defined in External Engagement section of External Engagement – Speaking Opportunity Policy to be followed for all communications**

6.2: Inquiry & Investigation

The FRM team will review and assess all the reported incidents of suspected fraud and carry out the required inquiries / investigations / inspections. FRM team may hire/involve the services of external / internal fraud investigation and / or forensic experts, wherever required. Further, all investigations will be handled on a case-by-case basis and may involve reporting to the Law Enforcements Authorities, where deemed necessary.

All investigations will be carried out objectively, and independently of the Line Management for the area in which the fraud has occurred or is suspected. All employees and third parties are required to provide complete support during all investigations.

FRM team will recommend and follow through the necessary disciplinary actions on case-by-case basis and learnings will be shared with relevant stakeholders to proactively manage and prevent similar cases in future.

6.3: Disciplinary Actions

Disciplinary action will be taken against the perpetrator(s) in the event of an incident of fraud, which may involve but not limited to suspension or termination of employment, penalty, criminal or civil action. The disciplinary actions will be decided on a case-by-case basis by the Head of FRM, HR and Legal in consultation with the CCO. Guidance will be obtained from the Risk Committee, where required

6.4: Safeguard

Confidentiality: FRM team maintains the confidentiality of all the information received. Results of investigation conducted shall not be disclosed to anyone other than those who have a legitimate need to know.

Bad faith allegations: Notwithstanding anything contained anywhere in this policy, the Company shall have the absolute authority to take disciplinary action against the informant if it is found, upon investigation, that the allegations were made by informant in bad faith.

7. AWARENESS

Employee awareness with respect to fraud is critical and it is important that all employees understand the reporting modes and their responsibilities.

All employees in managerial positions will be responsible for educating their team members on the importance of complying with Global Anti-Fraud Policy and identifying / reporting of suspicious activity, at all times.

Additionally, fraud awareness training and refresher programs will be carried out on an annual basis. The employees will go through computer-based training, declarations, and assessments with a passing score of 90%

8. REVIEW

The Global Anti-Fraud Policy will be reviewed and updated, as deemed necessary, by the FRM team on an annual basis