ANTI FRAUD POLICY

Navi General Insurance Limited

Document and Version Control

Revision Record

S.No.	Type of Information	Document Data
1.	Document Title	Anti-Fraud Policy
3.	Date of Release	19th January 2018
6.	Document Approvers	NAVI GI Board
7.	Document Owner	Risk Management & Compliance
8.	Document Author(s)	Risk Management

Document Approvers

S.No.	Approver	Approved Through / Nominee	Nominee Contact
1.	NAVI GI Board	Risk Management Committee	NA

Document Change History

Version No.	Nature of Change	Date Approved
1.0	First-time creation	19th January 2018
2.0	Annual Review without change	17th January 2019
3.0	Annual Review without change	23rd January 2020
4.0	Annual Review with changes	02nd February 2021
5.0	Annual Review with changes (changes reflected in Annexure B)	02nd February 2022
6.0	Annual Review with changes (changes reflected in Annexure B)	15th February 2023
7.0	Annual Review without change	21st May 2024
8.0	Annual Review without change	5th May 2025
9.0	Annual Review with changes to align with the IRDAI 2025 Guidelines	31st March 2026

1. Introduction

The Insurance Regulatory and Development Authority of India ("lRDAl") vide its Circular dated 9th October 2025 having reference No. IRDAI/IID/GDL/MISC/112/10/2025 has issued guidelines providing a regulatory framework for measures to be taken by Insurers and Distribution Channels to effectively address, manage, and mitigate risks arising from fraud. .
The Regulations 2024 read with Master Circular on Corporate for Insurers, 2024 issued by the lRDAl also requires insurance companies to set up a framework to monitor and implement Anti-Fraud Policy for effective deterrence, prevention, detection and mitigation of frauds in such a way that the insurance company is able to monitor risks across all lines of business on a continuous basis.

2. Objective

The objective of this Policy is to establish a comprehensive and robust fraud risk management framework that supports the Company's zero-tolerance approach to fraud. It seeks to effectively deter, prevent, detect, report, and remediate fraud across all operations by clearly defining management responsibilities and instituting structured procedures for timely identification and response to fraudulent activities.

The Policy further aims to promote a strong culture of integrity, safeguard policyholders' interests, protect the Company's financial stability, and uphold public trust. The framework is aligned with applicable regulatory requirements and industry best practices, following the principle of proportionality based on the nature, scale, and complexity of the Company's business and the evolving risk landscape.

3. Definition

- "Fraud", in general, is a willful act committed by an individual(s)/ entity (ies) by deception, misrepresentation, suppression, cheating or any other fraudulent means or illegal means thereby causing wrongful gain(s) to self or any other individual(s) and wrongful loss to the organization.
- "Insurance Fraud" (hereinafter referred to as 'Fraud') shall mean an act or omission intended to gain advantage through dishonest or unlawful means, for a party committing the fraud or for other related parties; including but not limited to:
    - Misappropriating funds;
    - Deliberately misrepresenting/concealing/not disclosing one or more material facts relevant to any decision / transaction, financial or otherwise
    - Abusing responsibility, position of trust or a fiduciary relationship.
- Red Flag Indicator or RFI means a possible warning sign, that points to a potential fraud and may require further investigation or analysis of a fact, event, statement, or claim, either alone or with other indicators.

4. Scope and Coverage

This policy and its related procedures apply to all staff, third party service providers, intermediaries and contractors of the Company and all channels of distribution including online sales. This policy shall cover following frauds:

- **Internal Fraud**: Fraud involving internal staff, including employees and/or senior management. This includes acts such as manipulation of internal records, overriding controls, misappropriation of funds, or collusion to bypass established processes for personal gain. It may also involve abuse of authority or privileged access to systems and information.
- **Distribution Channel Fraud**: Fraud involving distribution channels. This may include mis-selling of policies, falsification of customer information, unauthorized policy issuance, or manipulation of commissions and incentives by agents, brokers, or intermediaries. Such fraud may also involve collusion with customers or third parties.
- **Policyholder Fraud and/or Claims Fraud**: Fraud involving any person(s), in obtaining coverage or payment during the purchase, servicing, or claim of an insurance policy. This includes misrepresentation of facts at onboarding, submission of inflated or fictitious claims, and misuse of policy benefits. It may also involve staged events or concealment of material information to derive undue benefit.
- **External Fraud**: Fraud involving external parties' / service providers / vendors etc. This may include fraudulent activities by hospitals, garages, TPAs, surveyors, or other service providers through overbilling, provision of unnecessary services, document manipulation, or collusion with policyholders or employees.
- **Affinity Fraud or Complex Fraud**: Fraud involving collusion among one or more fraud perpetrators in the above categories. Such frauds are typically organized and may involve multiple stakeholders acting in coordination to exploit control gaps. These cases are often sophisticated in nature and may span across products, geographies, or processes.
- **Cyber or New Age Fraud:** Cyber or New Age Fraud refers to fraudulent activities carried out using digital platforms, technology, or the internet, with the intent to gain unauthorized access, manipulate information, or cause financial or reputational loss to the Company or its stakeholders. This includes activities such as phishing, hacking of systems, data theft, identity or credential compromise, and other technology-enabled threats.

5. Impact of Fraud

Fraudulent activities not only impact a Company's bottom line but also create reputational risks for the Company. Depending upon the type and extent of Fraud, the impact includes:

- Financial Loss
- Decrease in Profitability
- Negative publicity in press
- Deterioration in Stakeholder relations
- Increase in premium cost to customers
- Loss of Customers' trust
- Low employee morale

6. Governance Structure

The Company shall establish:

- Fraud Monitoring Committee (FMC)
    - Fraud Monitoring Committee (FMC) which shall be responsible for operationalizing the Fraud risk management framework within the insurer and oversee activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remedying.
    - Composition of the FMC:
        a) It should be headed by a KMP and include senior representatives from relevant departments, such as underwriting, claims, legal or any other department as deemed necessary.
        b) May form subcommittees, as required, for its effective functioning.
        c) Shall avoid conflicts of interest in its composition and functioning.
    - The MD & CEO shall constitute the FMC as per the anti-fraud policy comprising of at least three members from the senior management, preferably from the following members
        a) Chief Risk Officer / Head Risk Management
        b) Chief Financial Officer
        c) Head Human Resource
        d) Head Claims
        e) Company Secretary
        f) Chief Compliance Officer
        g) Appointed Actuary or Head Actuarial
        h) Head Operations
        i) Chief Underwriting Officer
    - The Committee shall meet minimum every quarter and, on an ad-hoc basis depending upon the responsibilities the committee is expected to discharge as per the Company's Anti-Fraud Policy.
- A Fraud Monitoring Unit (FMU), independent from internal audit, to support FMC in discharging its functions and effective implementation of measures suggested by FMC. The Company shall ensure availability of appropriate and adequate resources to the Fraud Monitoring Unit to carry out its functions effectively and manage cyber risks.

7. Roles and Responsibilities

Under the governance structure of the Company, various roles and responsibilities of various stakeholders, under this Policy, shall include the following:

7.1. Board of Directors

Board of Directors shall provide overall strategic oversight and governance for fraud risk management.
In particular, the Board of Directors shall be responsible for the following

- To set the “tone at the top” by fostering a culture of integrity, honesty, fairness, and openness across the Company as a foundation for effective fraud risk management.

- To approve the Company's Anti-Fraud Policy and any subsequent revisions thereto and ensure periodic review of the same.
- To provide overall strategic oversight of the fraud risk management framework and ensure alignment with the Company's risk appetite and governance standards.
- To review and monitor reports from the Audit Committee and Risk Management Committee on annual fraud risk assessment, fraud incidents, key trends, and material exposures, rather than focusing on operational thresholds.
- To seek insights on emerging fraud trends, status of significant investigations, and effectiveness of remedial actions taken by management to address control weaknesses.
- To ensure that adequate resources, systems, and governance structures are in place for effective fraud prevention, detection, and response.

7.2. Risk Management Committee

Risk Management Committee shall oversee implementation and effectiveness of the fraud risk management framework.
In particular, the Risk Management Committee shall be responsible for the following:

- To ensure effective implementation and oversight of the fraud risk management framework
- To review periodic reports from the Fraud Monitoring Committee (FMC), including its activities, findings, and recommendations including the financial impact of fraud on the insurer.
- To recommend corrective actions and improvements to the fraud risk management framework based on emerging risks and trends.
- To submit key findings and risk assessments to the Board.
- To monitor reports on external fraud cases, including those above defined materiality thresholds, irrespective of whether they result in financial loss.
- To monitor fraud risk exposure and emerging threats across business lines, products, and distribution channels.

7.3. Audit Committee

The Audit Committee provides oversight on financial integrity, internal controls, and fraud incidents with financial implications.
In particular, the Audit Committee shall be responsible for the following

- To evaluate the adequacy and effectiveness of internal controls, including controls designed to prevent and detect fraud.
- To review findings from Internal Audit relating to fraud and ensure timely remediation of control weaknesses.
- To oversee disciplinary actions in cases of internal fraud, where applicable.
- To monitor all internal fraud incidents, and external fraud incidents above defined materiality thresholds, and ensure appropriate action and closure.
- To review the financial impact of fraud incidents and assess implications on financial reporting and internal controls.

7.4. Fraud Monitoring Committee

The Fraud Monitoring Committee drives operational execution and monitoring of fraud risk management activities.

In particular, the Fraud Monitoring Committee shall be responsible for the following

- To operationalize the Fraud Risk Management Framework across the Company.
- To oversee fraud detection, investigation, reporting, and remediation activities.
- To ensure prompt action on suspected or confirmed fraud cases.
- To facilitate coordination with law enforcement agencies, regulators, and industry bodies.
- To conduct an Annual Comprehensive Fraud Risk Assessment to identify potential vulnerabilities across business lines and activities for fraud, using past experiences, emerging trends & Red Flag Indicators (RFIs), etc.
- To maintain records of all fraud instances and monitor trends.
- To maintain detailed records of all fraud incidents, including those above defined thresholds, and track their status, financial impact, and resolution.
- To analyze fraud trends, root causes, and control weaknesses, and report the same to the Risk Management Committee and Audit Committee, as applicable.
- To assess and quantify the severity and impact of identified fraud cases and recommend appropriate corrective, preventive, and punitive actions, including legal recourse, where required to Fraud Monitoring Unit.
- To recommend and periodically review measures to enhance the effectiveness of fraud risk management and strengthen internal controls across the Company.
- To identify functions, departments, products, and processes that are potentially vulnerable to fraud and recommend targeted mitigation measures.
- To facilitate coordination and information sharing with industry bodies (such as relevant councils/associations) and participate in industry-level fraud mitigation initiatives.
- To oversee mechanisms for receipt, review, and appropriate action on fraud-related complaints, including those received through whistleblower channels.
- To ensure timely and appropriate reporting of fraud cases to senior management, Board committees, and regulatory authorities, as applicable.
- To seek inputs, as required, from relevant functions such as Claims, Ethics, Information Security, Compliance, Risk Management, and Internal Audit for effective discharge of its responsibilities.
- To review and provide directions on corrective and preventive measures based on input from the Risk Management Committee (RMC) and ensure their implementation through the FMU.

7.5. Fraud Monitoring Unit (FMU)

The Fraud Monitoring Unit (FMU) supports day-to-day implementation, tracking, and reporting of fraud-related activities.

In particular, the FMU shall be responsible for the following:

- To implement and operationalize the Fraud Risk Management Framework across the Company in line with directions of the Fraud Monitoring Committee (FMC).
- To develop, implement, and periodically review the Fraud Risk Assessment Program, including methodologies for identification and assessment of fraud risks across the Company.
- To conduct periodic fraud risk assessments, identify fraud-prone areas, and define and maintain Red Flag Indicators (RFIs) for effective fraud identification
- To execute and ensure implementation of measures, recommendations, and action points approved by the FMC.
- To establish and maintain a centralized fraud incident database, ensuring completeness, accuracy, integrity, and availability of transaction-level details, actions taken, and case status.

- To monitor insurance claims, policy applications, and other business transactions using Red Flag Indicators (RFIs), analytics, and other tools to identify potential fraud risks.
- To analyze and track fraud trends, emerging typologies, and risk indicators across business functions, and report insights to the FMC and other relevant stakeholders.
- To undertake and manage end-to-end fraud investigations, including preliminary review, evidence gathering, documentation, and coordination with relevant departments, while ensuring independence and avoidance of conflicts of interest.
- To prepare detailed investigation reports for each fraud case, including findings, supporting evidence, and recommended corrective, preventive, and punitive actions, and submitting the same to the FMC.
- To coordinate and facilitate engagement with external investigation agencies and liaise with law enforcement agencies (LEAs), where required, in line with internal policies and FMC directions.
- To share investigation findings with Corporate Legal & Compliance for initiation of appropriate legal action, as applicable.
- To ensure timely identification, documentation, reporting, and escalation of suspected or confirmed fraud cases to FMC, Risk Management, and other relevant stakeholders.
- To prepare and submit periodic and ad-hoc fraud reports, including regulatory reporting inputs, to FMC, Risk Management Committee, Board, and regulatory authorities, as required.
- To establish and manage mechanisms for receipt, tracking, and resolution of internal and external fraud reports, including whistleblower complaints.
- To coordinate with internal functions to obtain necessary data, records, and support for fraud monitoring and investigation activities.
- To collaborate and liaise with industry bodies, industry peers, regulators, and other external stakeholders for fraud intelligence sharing and case follow-up.
- To design and drive awareness, training, and communication initiatives for employees, intermediaries, and other stakeholders to strengthen fraud prevention and detection capabilities.

7.6. CEO & Functional Heads

The CEO & Functional Heads will ensure policy implementation and embed fraud risk controls within business operations. In particular, the CEO & Head of the Departments shall be responsible for the following:

- To ensure implementation of the Anti-Fraud Policy and Fraud Risk Management Framework within their respective functions.
- To set the “tone at the top” by promoting a culture of integrity, ethical behavior, and zero tolerance towards fraud across their functions.
- To establish and maintain effective internal controls, in coordination with the Risk Management function, for identification, detection, prevention, and mitigation of fraud risks.
- To identify sensitive roles and define clear delegation of authority and approval thresholds to mitigate fraud risk.
- To ensure fraud risk assessment is embedded within their respective functions and to consider fraud risks while introducing new products, processes, or business activities.
- To encourage a strong anti-fraud culture by enabling employees and stakeholders to report suspected fraud without fear of retaliation.
- To ensure timely identification, reporting, and escalation of suspected or actual fraud incidents to the appropriate forums, in line with the Company’s reporting framework.

- To review and monitor fraud risk reports, investigation outcomes, and control effectiveness within their respective functions.
- To ensure adequate resources, systems, and training programs are in place to support effective fraud risk management, including periodic awareness for employees and relevant stakeholders (including distribution channels, where applicable).
- To ensure that the Fraud Monitoring Unit (FMU) is adequately staffed, skilled, and resourced to effectively discharge its responsibilities.
- To ensure appropriate due diligence and background verification processes are carried out for employees, intermediaries, vendors, and other associated parties.
- To cooperate with investigation processes and support relevant functions by providing required information and access, as per applicable policies and procedures.

To ensure compliance with applicable regulatory requirements, internal policies, and standards relating to fraud risk management.

7.7. Internal Audit

The Internal Audit shall carry out the following responsibilities in connection with internal fraud:

- To independently assess the adequacy and effectiveness of the Fraud Risk Management Framework.
- To identify control gaps and recommend corrective actions.
- To review compliance with Anti-Fraud Policy and applicable regulatory requirements.
- To report findings to the Audit Committee.
- To validate closure of audit observations and remediation actions.

7.8. Ethics Committee

The Ethics Committee shall carry out the following responsibilities in connection with fraud:

- To administer whistleblower policy and reporting channels.
- To ensure confidentiality and protection of whistleblowers.
- To review complaints received through whistleblower channels.
- To facilitate appropriate routing and investigation of complaints.
- To monitor resolution and closure of reported concerns.
- To take action in cases of misuse or malicious reporting.

Upon receipt of any instance of internal (actual or suspected) fraud or violations of the code of conduct of the Company, based on the nature & severity of the case, the committee may refer the case for further investigation to the FMU.

7.9. Compliance & Legal

The responsibilities of Compliance & Legal shall include the following

- To adhere to the Anti-Fraud Policy and Code of Conduct and ensure alignment with applicable laws and regulatory requirements.
- To provide secretariat and governance support to the Fraud Monitoring Committee (FMC), including documentation, record-keeping, and tracking of decisions/actions.

- To remain vigilant and ensure that suspected or observed frauds are appropriately reported through designated channels and escalated as required.
- To assess sufficiency of evidence in fraud cases and advise on initiation of legal proceedings, including engagement with law enforcement agencies, where required.
- To initiate and manage legal action in fraud cases, including coordination with external counsel and law enforcement agencies.
- To ensure timely and accurate regulatory reporting of fraud cases, including submission of prescribed returns (e.g., FMR returns or equivalent) to the regulator within defined timelines.
- To provide inputs and support for regulatory disclosures, filings, and correspondence related to fraud incidents.
- To cooperate fully in investigations and provide legal guidance to ensure adherence to applicable laws and evidentiary standards.
- To avoid conflicts of interest and ensure ethical practices in handling fraud-related matters.
- To support development and review of policies and procedures to ensure compliance with evolving regulatory requirements related to fraud risk management.
- To participate in and support fraud awareness and training initiatives from a regulatory and legal perspective.
- To protect confidentiality of information and ensure appropriate handling of sensitive and privileged information.

7.10. Employees

All employees act as the first line of defense by adhering to policies and reporting suspicious activities. In particular, the responsibilities of employees shall include the following:

- To adhere to the Anti-Fraud Policy and Code of Conduct.
- To remain vigilant and report any suspected or observed fraud through designated channels.
- To cooperate fully in investigations and provide required information.
- To avoid conflicts of interest and unethical practices.
- To participate in training and awareness programs on fraud prevention.
- To protect confidentiality of information and prevent misuse of company assets.

7.11. Framework for Exchange of Information

The Company shall closely work with market participants, industry players and the Regulator and promote multiple avenues to enhance mutual cooperation and best practice exchange.

8. Fraud Risk Identification, Mitigation and Monitoring

8.1. Fraud Identification

- The Company shall establish and maintain a robust framework for timely identification of fraud risks across all business lines, products, processes, and distribution channels. Such identification shall be risk-based and consider historical incidents, emerging fraud typologies, fraud trends, business volumes, and inherent risk exposures.

- Fraud risk identification shall be an ongoing process and shall be supported by periodic Fraud Risk Assessments conducted across the Company. The Fraud Monitoring Committee (FMC) shall design and implement the Fraud Risk Assessment Program, with oversight from the Risk Management function and support from relevant business and control functions.
- The Company shall define and implement appropriate Red Flag Indicators (RFIs) and other detection mechanisms to facilitate early identification of potential frauds. Such indicators shall be embedded within systems, processes, and transaction monitoring frameworks and shall be periodically reviewed and updated to remain relevant and effective.
- The Company shall ensure that fraud identification mechanisms are integrated within business operations, including product design, underwriting, claims management, and distribution processes, with support from relevant business and control functions.
- Appropriate mechanisms, including internal reporting channels and a Whistleblower Policy, which incorporates provisions for whistleblower protection, shall be established to enable timely reporting and identification of suspected frauds.
- All directors, employees, and associated parties shall disclose any potential or actual conflicts of interest in business transactions or relationships that may pose a risk of fraud or misconduct.

8.2. Fraud Prevention and Mitigation

- The Company shall implement appropriate preventive and detective controls to mitigate identified fraud risks, ensuring that such controls are aligned with each category of fraud, including internal distribution channel, policyholder/claims, and external frauds. The FMU shall ensure that adequate control measures are designed and operating effectively across all functions to prevent and detect fraud.
- The Company shall establish and maintain a robust cybersecurity framework / policy and continuously strengthen systems, access controls, and monitoring mechanisms to mitigate risks arising from cyber or new age frauds.
- The Company shall establish robust monitoring and review mechanisms to ensure the ongoing effectiveness of fraud risk management practices. This shall include:
    - Maintenance of a centralized Fraud Incident Database, capturing details of suspected, attempted, and confirmed frauds, including blacklisted entities
    - assess compliance with the Fraud Risk Management Framework
    - Continuous monitoring of distribution channel activities and trends to identify unusual patterns or anomalies
- Ongoing oversight of vendor and third-party activities to ensure adherence to contractual and fraud prevention requirements
- Analysis of customer complaints and grievances to identify potential fraud indicators or systemic weaknesses
- The Company shall implement structured and periodic training, education, and awareness programs to strengthen fraud prevention and detection capabilities across the organization and its ecosystem. Such programs should be designed to:
    - Educate employees, senior management (including Board members), and distribution channels on fraud risks, red flag indicators, and emerging fraud trends
    - Provide clear guidance on identification, reporting, and escalation procedures for suspected fraud

- Reinforce the importance of ethical conduct, vigilance, and adherence to the Anti-Fraud Policy

  In addition, the Company should conduct regular fraud awareness initiatives for policyholders and the general public to enhance awareness of fraud risks and promote preventive measures. The training and awareness programs shall be conducted periodically and updated as necessary to remain aligned with evolving fraud risks and regulatory expectations.

- The Company shall as part of the fraud prevention process carry out due diligence and background verification of its employees, staff, and insurance agents/ Corporate Agent/intermediaries/ TPAs, as applicable. The due diligence for employees and staff shall be carried out by the HR function as mentioned in section 7.2. The due diligence for other third parties should be carried out in the same manner as that for outsourcing vendors.
- The Company shall knowingly not engage in any business/contractual relationship with people of criminal record or convicted by a competent court of law.

Exit interviews shall be conducted for employees leaving the organization regardless of their position to identify potential fraud.

8.3. Fraud Detection and Investigation

- The Company shall establish multiple reporting channels for identification and reporting of suspected fraud managed internally or by authorized third parties.
- The Company shall ensure that all reported incidents are appropriately acknowledged, recorded, and, where required, additional information is sought from the complainant to facilitate further review.
- In respect of customer (claims) fraud, the Company shall ensure that all claims (cashless and reimbursement) are subject to preliminary validation checks, including verification of customer KYC, policy validity, and hospital empanelment status, prior to further processing.
- The Company shall deploy AI/ML based fraud propensity models to evaluate all eligible claims and assign risk ratings (such as High, Medium, or Low) along with supporting rationale.
- The Company shall adopt a risk-based approach for claims handling, wherein claims assessed as high risk shall be subject to detailed investigation, while other claims shall be processed in accordance with their risk profile. Investigations may be conducted through internal teams or empaneled external agencies, with appropriate documentation and quality assurance oversight.
- The Company shall classify suspected fraud incidents based on nature and assign them to the relevant investigator for further handling.
- All claims shall be subject to final determination by an authorized adjudicating authority, who shall be enabled with relevant information including risk assessment outputs, investigation findings, historical data, and internal intelligence inputs, and shall have the discretion to seek additional information prior to decision-making
- In respect of reimbursement claims, the Company shall apply the same risk-based principles, with enhanced reliance on document-based verification and post-facto quality assurance reviews.
- In respect of internal and vendor-related frauds, the Company shall undertake investigations upon receipt of complaints through designated reporting channels. The investigation process shall include collection of information, review of documents, interviews with relevant individuals, and obtaining supporting evidence. This introduces a structured investigation lifecycle specific to internal and third-party frauds, distinct from claims processing.

- The Company shall ensure that individuals against whom allegations are made are provided an opportunity to respond, including issuance of a show-cause notice and provision of reasonable timelines for response. This formalizes principles of natural justice within the investigation process.
- Based on the investigation findings, the Company shall constitute a disciplinary committee comprising representatives from relevant functions (including Human Resources and Legal, at a minimum) to evaluate the case. The concerned individual may be required to appear before the committee for further clarification. This introduces a formal governance layer for decision-making in internal and vendor fraud cases.
- The disciplinary committee shall review all evidence, responses, and representations, and recommend appropriate corrective and/or disciplinary actions in line with the Company's Code of Conduct and applicable policies.
- The Company shall ensure that all investigations, decisions, and actions taken are adequately documented and retained in accordance with applicable requirements.
- The Company shall establish a feedback mechanism to facilitate continuous improvement, including strengthening internal controls and refinement of fraud detection mechanisms based on investigation outcomes.
- The Company shall periodically review cases of fraud and near-misses to identify missed detection opportunities and strengthen controls and detection mechanisms.
- The Company shall ensure that all activities relating to fraud reporting, assessment, and investigation are conducted in a confidential manner, with due regard to fairness, objectivity, and protection of whistleblowers. This extends confidentiality and protection principles uniformly across both claims and internal/vendor fraud processes.
- No unfair treatment shall be given to a person who has reported in good faith any suspected or alleged incidence of fraud and there shall be no discrimination, harassment, victimization, retaliation, threat against such person.
- The identity of the person who has reported the suspected or alleged incident of fraud shall be kept confidential to the extent possible and permitted under the law.
- However, any abuse of this protection (for example, any false or bogus allegations made by a person knowing them to be false or bogus or with a mala fide intention) will warrant disciplinary action.
- If an employee or an officer reports a suspected or alleged incident of fraud for personal gain or disrupts the working environment of the company with mala fide intention, such employees would not get any protection and appropriate action shall be taken by the Company against such employee.
- The Company shall establish a detailed Fraud Investigation Standard Operating Procedure (SOP) to govern the end-to-end investigation lifecycle, including case intake, triaging, investigation, evidence gathering, documentation, and closure. The SOP shall define internal turnaround timelines (TATs), escalation and reporting protocols, and clearly identify designated roles and nodal officer(s) responsible for fraud reporting and coordination. It shall also outline appropriate disciplinary, contractual, and legal actions against fraud perpetrators, as well as actions for non-compliance with the Fraud Risk Management Framework. The SOP shall be reviewed periodically to ensure alignment with regulatory requirements and evolving fraud risks.

9. Internal Reporting

- Every instance of attempted fraud or detected actual fraud (regardless of whether it has caused actual financial loss to the Company at that juncture or not) shall be reported without delay by the affected department/operational unit/any person having knowledge, to the FMU or the Ethics team.
- Fraud Monitoring Unit (FMU) should report every fraud instance to FMC every month.
- The FMC shall submit quarterly reports to the RMC on its activities, findings, and recommendations, including the financial impact of fraud on the insurer.
- The FMC shall submit report of the Annual Comprehensive Fraud Risk Assessment before the Board of Directors through RMC.
- The FMC shall report to the Audit Committee, in addition to the RMC, in case of all internal frauds.

10. Reporting to the Authority

- The Company shall report incidents of fraud to Law Enforcement Agencies and/or other relevant agencies subject to applicable laws
- The Company shall file annual returns with Authority in forms FMR-1 within 30 days of close of the financial year.
- In the event of fraud committed by distribution channels registered by IRDAI, The Company shall promptly escalate and report the matter to IRDAI without delay.

11. Coordination with Law Enforcement Agencies

- Perpetration of a Fraud or an attempt to commit a fraud is a serious issue, which will be dealt with swiftly by the company.
- Instances where sufficient evidence of fraud is obtained post conduct of internal investigations / review would be reported to the relevant law enforcement agencies in consultation with the appropriate authority.
- Employees / Intermediaries shall cooperate with any law enforcement agency in order to facilitate the expeditious completion of investigation.

12. Leveraging and Sharing Threat Intelligence with Insurance Information Bureau (IIB)

- The Company shall actively liaise with the Insurance Information Bureau (IIB) and participate in the Fraud Monitoring Technology Framework, as applicable, to ensure effective utilization of industry-wide data for prevention and detection of fraud.
- The Company shall contribute to and leverage the centralized database maintained by IIB for timely sharing and receipt of threat intelligence relating to attempted, suspected, and confirmed fraudulent activities across the insurance sector.

- The Company shall adopt appropriate mechanisms, including use of unique identifiers, to enable accurate identification of policyholders across insurers and enhance the effectiveness of fraud detection measures.
- Further, the Company shall report to IIB details of blacklisted entities, including distribution channels, hospitals, third-party vendors, and identified fraud perpetrators, in accordance with prescribed procedures and timelines, to support the maintenance of a caution repository and safeguard the integrity of the insurance ecosystem.

13. Compliance

The Company shall ensure that all employees, intermediaries, vendors, and other stakeholders adhere to this Policy. Any non-compliance shall be treated as a violation of applicable terms of employment, engagement, or contract, and shall attract appropriate disciplinary, contractual, or legal action, as applicable. All employees and officers shall promptly report any suspected or actual fraud through designated channels, and functional heads shall ensure adequate controls within their respective areas to prevent and detect fraud. This Policy shall be adequately communicated to all relevant stakeholders, and failure of external parties to adhere to the same may result in appropriate action, including termination of engagement.

14. Recovery of Fraud Losses

The Company shall take all reasonable and necessary steps to recover losses arising from fraud. Upon detection of fraud, the concerned functions shall initiate appropriate loss mitigation and recovery actions, including recovery from employees, customers, policyholders, intermediaries, vendors, or other involved parties, as applicable. Such actions may include adjustment, set-off, withholding of payments, and initiation of legal proceedings, including recovery suits, wherever feasible, in consultation with the Legal function.

15. Custodian of the Policy

The Chief Risk Officer (CRO) of the Company shall be the custodian of the Policy.

16. Monitoring and Review

- The Head of FMU shall monitor the implementation of the policy and shall provide an assurance to the FMC and RMC at least annually, for effective deterrence, controls, prevention, detection and mitigation of frauds.
- The Head of FMU will review the policy at least annually in line with the Company Business, Products and Process and shall align with the amendment in the Regulatory Guidelines from time to time. Any revised version shall be submitted to the FMC and RMC for its review and further recommendation to the Board of Directors for approval.

17. Related Documents

- Fraud Prevention procedure
- Whistleblowing policy
- Fraud Detection Procedure
- Fraud Investigation and Response Procedure