ANTI FRAUD POLICY
Liberty General Insurance Limited

Version No	Date of Review/Approval	Approved by
Version I	7th May 2013	Board of Directors
Version II	6th May 2014	Board of Directors
Version II	8th May 2015	Board of Directors
Version II	27th May 2016	Board of Directors
Version III	10th May 2017	Board of Directors
Version IV	11th May 2018	Board of Directors
Version IV	8th May 2019	Board of Directors
Version V	27th May 2020	Board of Directors
Version V	21st May 2021	Board of Directors
Version V	13th May 2022	Board of Directors
Version V	15h May 2023	Board of Directors
Version VI	7th November 2023	Board of Directors
Version VI	7th June 2024	Board of Directors
Version VII	15th May 2025	Board of Directors
Version VIII	18th May 2026	Board of Directors

LIBERTY GENERAL INSURANCE LIMITED – ANTI FRAUD POLICY

1. PREAMBLE / REGULATORY REFERENCE

This Anti-Fraud Policy is framed as per the Insurance Regulatory and Development Authority of India (Insurance Fraud Monitoring Framework) Guidelines, 2025 [Ref No: IRDAI/IID/GDL/MISC/112/10/2025] dated 9th October 2025 ("2025 Guidelines") which provides a regulatory framework on the measures to be taken by the Company to address and manage risks emanating from fraud.

Accordingly, the Anti-Fraud Policy lays down the framework adopted by the Company to implement mitigation measures and pro-active fraud detection framework.

LGI is committed to establishing and maintaining an organizational culture that supports ethical conduct, thereby minimizing the risk of fraud. The introduction of an effective fraud control policy is an essential element specifically designed to ensure the Company maintains the ability to operate with integrity, transparency and at maximum economic efficiency. Implementing effective fraud controls is part of effective corporate governance and management practices. Such controls seek to protect LGI's assets, interests and reputation.

2. SCOPE & PURPOSE / OBJECTIVE

Scope of the Policy includes:

a. Providing an understanding of 'Fraud' and its implications and effects on the Company and ensuring that the management is aware of its responsibilities for the determent, detection and prevention of fraud.

b. Providing clear guidance on how determent, detection, prevention and investigations into fraudulent activities will be conducted and ensuring protection of those who report frauds in line with the 'Protected Disclosure' clause (as per the 'Whistle blower policy').

c. Ensuring consistent and effective investigation, reporting and disclosure of fraud occurrences. Providing assurance that the potentially fraudulent activities will be duly investigated and dealt with appropriately. Setting the tone that fraud is not acceptable and shall not be tolerated.

d. Ensuring processes to deter, prevent, detect, manage and report frauds as well as ensuring that the preventive measures are continuously enhanced, strengthened and implemented in a speedy manner.

Objective of the Policy:

a. To establish a comprehensive Fraud Risk Management Framework to deter, prevent, detect, report and remedy the incidences of frauds and other irregularities.

b. To enhance the Company's resilience against fraud, foster a culture of integrity, protect policyholders' interests, safeguard financial stability and maintain public trust.

c. Promote zero tolerance towards fraud across organization

3. APPLICABILITY

The Policy will be applicable to all employees and officers of the Company, Board of Directors, contractual staff, trainees, agents, insurance intermediaries, service providers, consultants, vendors, policy holders, contractors and sub-contractors, associated with the Company.

4. KEY DEFINITIONS

4.1 Fraud:

A. 'Insurance Fraud' ('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.

B. Fraud may also include any other non-compliances to the Companies code of conduct; online frauds; cyber-attacks; any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the Company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss.

4.2 Terminologies used in the policy:

A. "Company" means "Liberty General Insurance"
B. "Employee" means any person employed by the Company (probationer, confirmed or outsourced), including former employee and Directors of the Company (whether working in India or abroad).
C. "Fraud Monitoring Committee" means the Committee formed by the Board of Directors in accordance with the provisions of 2025 Guidelines consisting of such members as may be determined by the Board of Directors from time to time. The Committee shall discharge its responsibilities as may be assigned by the Board of Directors.

D. "Policy or This Policy" refers to the 'Anti-Fraud Policy'
E. "Risk & Loss Mitigation Team (RLM)" means the unit formed to handle, fraudulent activities specifically for the claims & policy holder frauds.
F. "Suspect individual" means the individual or representative of an entity potentially involved in perpetrating the fraud.
G. "Red Flag Indicator (RFI) or Triggers" 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.
H. "Cyber or New Age Fraud" means any insurance fraud carried out using digital or new age technologies.
I. "Distribution Channels" include insurance agents, intermediaries or insurance intermediaries,
and any persons or entities authorized by the Authority to involve in sale and service of insurance
policies.
J. "Intermediary or insurance intermediaries" include insurance brokers, re-insurance brokers, insurance consultants, corporate agents, third party administrators, surveyors and loss assessors and such other entities, as may be notified by the Authority from time to time

5. COVERAGES & DESCRIPTION OF POLICY

5.1 Classification or Types of Fraud:

The categories described below are illustrative & not exhaustive. New or emerging fraud patterns, including those arising from technological advancements, shall also fall within the ambit of this Policy.

A. Internal Fraud:
Fraud involving internal staff, including employees and/or senior management.

B. Distribution Channel (Intermediary) Fraud:
Fraud perpetuated or involving Distribution Channels.

C. 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.

D. External Fraud:
External Fraud refers to fraudulent acts committed by external parties / vendors / service providers etc.

E. Affinity Fraud or Complex Fraud:
Fraud involving collusion among one or more fraud perpetrators in the above categories.

5.2 Appendix A provides a representative list of fraudulent acts/omissions/ red flag indicators under each of these broad categories.

5.3 Fraud Risk Management Framework

The Company shall adopt appropriate fraud risk management framework sensitive to its business profile to enable it to deter, prevent, detect, report and remedy insurance frauds. The fraud risk management framework shall be specific to the business considering the nature of business, size, risk profile, overall business strategy, products, distributions channels, technology infrastructure, and any other applicable parameter including various activities carried out by the Company.

The Risk Management Committee ("**RMC**") shall be responsible for effective implementation and oversight of the fraud risk management framework**.** The Fraud Risk Management Framework shall consist of following components:

5.4 Fraud Monitoring Committee ("FMC")

a) FMC shall be responsible for operationalizing the Fraud risk management framework within the Company and oversee activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remedying.

5.5 Composition of FMC

a) The FMC shall comprise the following: –
   1. Chief Risk Officer (Chairperson)
   2. Chief Compliance Officer
   3. Chief Financial Officer
   4. Head of Claims
   5. Head of Human Resources
   6. Head of Commercial Underwriting

b) The Head of the Fraud Monitoring Unit shall serve as the permanent invitee of the Fraud Management Committee.

c) The FMC may form subcommittees, as required, for its effective functioning. The Committee may invite other officers as invitees or as may be mandated under any other regulations.

d) Minimum 3 members in person or audio/video call shall constitute quorum for the conduct of Meetings. The Committee shall hold its Meetings at least once in a quarter or such other shorter intervals as may be required.

e) The Chairperson may determine any potential conflict of interest with respect to functioning of the FMC and excuse any member from attending any meetings of FMC to ensure fair decision making by FMC.

5.6 Role and functions of FMC

The FMC shall, inter-alia be responsible to:

a) Recommend and regularly update, based on experiences, appropriate measures on fraud risk management to various functions.
b) Oversee prompt responses to instances or suspicions of fraud.
c) Maintain all relevant details pertaining to each instance of fraud.
d) Facilitate collaboration with industry peers / bodies, law enforcement agencies and regulatory bodies to pursue cases of fraud and share information / intelligence on known fraud schemes and perpetrators.
e) 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. and report to the Board of Directors through RMC.
f) Identify areas for improvement and adaptation of the Fraud Risk Management Framework.
g) Recommend disciplinary actions against employees involved in frauds / fraudulent activities.
h) Oversee the implementation and effectiveness of this Policy and Fraud risk management framework and recommend to RMC.
i) Review Red Flag Indicators (RFIs) regularly for their continued relevance and effectiveness in detecting fraud.
j) Submit quarterly reports to the RMC on its activities, findings, and recommendations, including the financial impact of fraud on the Company.
k) Report to the RMC and Audit Committee, in case of all internal frauds/complaints/investigations.
l) For all closed cases, review the systems and procedures, identified the causative factors and plugged the lacunae and the fact of which shall be taken note of and recommended to Audit Committee.
m) Form subcommittees, as required, for effective functioning.
n) Undertake other such actions, as may be required as per the Regulatory provisions.

o) Supervising and monitoring matters reported using the Company's whistle blowing or other confidential mechanisms for employees and others to report ethical and compliance concerns or potential breaches or violations and ensuring investigations are conducted in a timely manner and in accordance with procedure.
p) Carry out such other activities as may be assigned by the RMC / Board from time to time.
q) Issue and maintain a Fraud Control Procedure (Fraud Risk Identification, Mitigation, Monitoring & Reporting, Protection).
r) operationalizing the Fraud Risk Management Framework within the Company and oversee activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remedying.
s) Monitoring & directing proactive compliance with external laws and regulations and internal policies, including its code of ethics or conduct.
t) Put adequate controls in place to identify weaknesses, lapses, breaches, or violations to help detect and address the same.
u) Advising the Board on the effect of the above on the Company's conduct of business and helping the Board set the correct "tone at the top" by communicating, or supporting the communication, at all levels of the Company of the importance of ethics and compliance.
v) Ensuring there is an on-going fraud awareness program, including training for Management and staff in relation to their responsibilities for preventing, detecting, and reporting fraud.

5.7 Fraud Control Procedures (Fraud Risk Identification, Mitigation, Monitoring & Reporting):

The FMC will issue and maintain a Fraud Control Procedure that will outline the following:

A. **Procedures for Fraud Monitoring**:
Procedures to identify, deter, prevent, detect, investigate, and report insurance frauds. The procedures will also define how fraud information flows between various departments of LGI. In line with IRDAI Guidelines on Insurance e-commerce dated 9th March 2017, the Company's Self-Network Platform (online portals) shall have a pro-active fraud detection policy for the insurance e-commerce activities, and it shall deploy necessary applications/procedures for the purpose of
   i Detecting and identifying frauds
   ii Follow-up mechanism for prosecuting persons who committed frauds.
   iii Cooperation amongst market participants to identify frauds.
   iv Building a database of those committing frauds and sharing with other market participants

To ensure objectivity and fairness, FMC Members with any conflict of interest or bias be excluded from the FMC meetings when making decisions on fraud matters. This may include FMC Members who have a personal or financial interest in the outcome of the decision or who were part of fraud investigation or close relationship with the parties involved in the fraud investigation. This shall ensure objective and credible decision-making by FMC.

B. Identification:

Identify Potential Areas of Fraud – Identify areas of business and the specific departments of the organization that are potentially prone to fraud and lay down a detailed department-wise, anti-fraud procedures. These procedures lay down the framework for detection, prevention and identification of fraud and mitigation measures by putting in place appropriate measures to identify and assess fraud risks. Based on the line of business, activities, experience, trends etc. Company shall identify RFIs, as applicable, for detection of frauds and incorporate them appropriately in their operations, as approved by the FMC. Such RFIs shall be reviewed regularly for their continued relevance and effectiveness in detecting fraud.

C. Mitigation & Prevention of Frauds:

- Due Diligence Procedures to carry out the due diligence on the personnel (management and employees) / insurance agent / vendors at the time of appointment / engagement.
- Regular Communication – Procedures for fraud mitigation communication within and outside the organization at periodic intervals and/or ad hoc basis, as may be required.
- Client Communication – Procedures to inform both potential and existing clients about LGI's anti-fraud policies including necessary caution in the insurance contracts/ relevant documents, highlighting the consequences of submitting a false statement and/or incomplete statement, for the benefit of the policyholders, claimants and the beneficiaries.
- Co-ordination with Law Enforcement Agencies – Procedures to coordinate with law enforcement agencies for reporting frauds on timely and expeditious basis and follow-up processes thereon.
- Framework for Exchange of Information - Procedures for exchange of necessary information on frauds through the Council of General Insurers.
- In order to ensure the identified fraud risk are mitigated, the Company shall put in place appropriate control measures with respect to each category of fraud.
- Conduct regular fraud awareness programs to educate policyholders and the general public about the risk of fraud and how to prevent and protect against it.

- Conduct, as appropriate, periodic training programs tailored to the functions of employees, senior management, board members, and Distribution Channels.
- A brief training on prevention of frauds shall be imparted to all new entrants during the induction training.
- All employees shall be required to confirm their adherence to this Policy and declare any Conflict of Interest, once in a year.
- In order to prevent Cyber or New Age fraud, establish and implement robust cybersecurity framework, through Infosec Department / Chief Information Security Officer (CISO), to protect against evolving cyber frauds or threats and continuously monitor and strengthen systems and processes for fraud risk management, such as incident databases, customer verification, and access control. The infosec Department / CISO shall utilize a team with relevant risk and technological expertise to manage cyber fraud risks across various business lines
- Reduce exposure to fraudulent claims pertaining to its reinsurance business by understanding the fraud risk management systems of its counterparties to ensure the implementation of effective policies and controls.
- To ensure a comprehensive approach to fraud prevention, it is essential that Distribution Channels (other than Intermediaries and Insurance Intermediaries) shall comply with the Company's anti-fraud policies, procedures and controls. The Distribution Channel (other than Intermediaries and Insurance Intermediaries) shall inform the Company and provide all relevant details in the event of any suspicion of fraud.
- Review of Missed Insurance Fraud Detection Opportunities: Following any detected fraud event, conduct a post-incident review to understand the reason of fraud and undertake implementing improvements to the existing process, if required

D. Monitoring:

- Maintain an Incident Database (Repository) of persons convicted of or attempting fraud,
- Conduct fraud-sensitive audits, in consultation with the Audit Committee, for compliance with the Fraud Risk Monitoring Framework,
- Track business trends from distribution channels,
- Continuously monitoring vendor activities for compliance with fraud prevention measures and contractual obligations
- Analyse customer grievances & complaints to detect & prevent frauds
- The Company shall participate in the Fraud Monitoring Technology Framework made available by the Insurance Information Bureau (IIB) and share with IIB, details of claim & policy related frauds, details of distribution

channels, hospitals, third party vendors and fraud perpetrators blacklisted) to safeguard integrity of the insurance sector by preventing the involvement of those with a record of fraudulent activities & help the industry combat fraud.

E. Reporting:

- LGI shall report statistics on various fraudulent cases which come to light and action taken thereon to IRDAI, in Form FMR -1 within 30 days of the close of the financial year i.e. by April 30 every year.
- Co-ordination with Law Enforcement Agencies –The Company shall coordinate with law enforcement agencies for reporting frauds on timely and expeditious basis and follow-up processes thereon.
- In the event of fraud committed by Distribution Channels registered with IRDAI, the Company shall promptly escalate and report the matter to IRDAI without delay

F. Protection:

FMC shall be responsible for protection of the persons who intimate or raise concerns in relation to the possible fraud from any adverse treatment by any other person(s) within or outside the organization, in accordance with the Board approved Whistle Blower Policy of the Company.

5.8 Roles and Responsibilities:

To help ensure that LGI's fraud prevention and risk management program is effective, it is important to understand the roles and responsibilities that personnel at all levels of LGI have with respect to fraud management. The Executive Management, Employees and Fraud Monitoring Unit have roles in LGI's fraud management program.

a. **Fraud Monitoring Unit (FMU):** The primary administration of the functions of the FMC will rest with the FMU, who will have adequate resources, including data availability to carry out the same in coordination with the various functional heads. The function may delegate tasks to relevant officers for assistance with or participation in all fraud or suspected fraud investigation related to employee dishonesty or any other fraud. Depending on the requirement and subject to appropriate due diligence, FMU may, in consultation with FMC, seek support from external experts in complicated matters.

   The FMU, shall function independent from internal audit function, under the guidance and oversight of the FMC, and in accordance with the Fraud Risk Management Framework would discharge its functions including those listed below, towards ensuring a zero-tolerance approach toward fraud:

   - To put in place Fraud Monitoring Framework, in consultation with FMC and RMC, that appropriately measures to identify and assess fraud risks.

- To identify potential areas of frauds and formulate RFIs
- To evaluate and review Red Flag Indicators periodically (at least annually).
- To put in place control measures with regards to frauds
- Monitor and maintain an incident database of persons convicted or attempted fraud conducting fraud sensitive audits for compliance with Fraud Risk Monitoring Framework
- Track business trends from distribution channels, continuously monitoring vendor activities for compliance with fraud prevention measures and contractual obligations
- Analyze customer grievances and complaints to detect and prevent fraud.
- Endeavor to complete the fraud identification to remedy within 30 days, any extension beyond this period may be subject to review and approval by FMC
- Supervising and guiding investigations into frauds and whistleblower complaints, and reviewing outcomes thereof
- Ensuring appropriate, corrective, disciplinary, preventive and remedial actions are taken based on investigation findings

b. **Risk and Loss Mitigation Team (RLM)**: The RLM Team shall be responsible for handling all Claims & policy holder Frauds.

c. **Internal Audit Function**: FMU shall notify the Head of Internal Audit immediately of any employee fraud or suspected employee fraud matters identified post preliminary investigation and shall provide periodic updates on the investigation on an ongoing basis, at a minimum on a quarterly basis, until the matter is fully concluded.

d. **Human Resources Function**: In addition to initiating action against employees as recommended by the FMC will ensure all employees are aware of the Anti-Fraud Policy through induction training and regular communication of policy updates. In cases of suspected involvement of employees in frauds, Human Resources Department shall play an active role through the process of investigation. HR shall, under the guidance of FMC, issue show cause notice to employees under investigation to obtain their response whenever substantial evidence is found against them. FMU shall present the outcome of the investigation to the FMC.

e. **Function Heads:** It is the responsibility of the function heads to ensure that mechanisms are in place that minimize the opportunity for fraud and dishonesty within their area of control. Function heads are responsible for implementing any actions required /suggested by the FMC. Function Heads are also responsible for ensuring that persons who raise concerns in relation to possible fraud are protected from any adverse treatment or retaliation.

f. **Compliance Officer:**

Compliance Officer is responsible for the following:

- Liaison with Regulatory Authority on fraud reporting requirements
- Furnish various reports on frauds to the Regulatory Authority as stipulated in this regard

g. Depending on the requirements, the FMC may direct any other employee / department of the Company to ensure implementation of any actionable

5.9 Responsibilities, delegation of authorities for all relevant functions including for identified sensitive posts

• Chief Risk Officer (CRO) – responsible for overall fraud risk oversight.
• Finance / Treasury / Accounts Payable – responsible to report cases of financial fraud
• Claims – to report fraud cases based on claim data analysis for region/zone wise
• Underwriting – fraud Risk Identification before accepting risk
• Investigation & Fraud Control Unit (IFCU) – manage fraud detection, investigations, and
reporting.
• Compliance – enforce regulatory norms
• Internal Audit – conduct fraud-sensitive audits and internal checks
• IT Security– cyber controls and report cyber fraud
• Procurement / Vendor Management – report fraud cases • Operations – quality control and report fraud cases

5.10 Intimating the Frauds:

- Information on suspected frauds and fraudulent methods used can be reported by the employees or third parties or other stakeholders to the following:
  a. Write email to antifraud@libertyinsurance.in
  b. Letter / Email addressed to the FMC or any member thereof.

5.11 Investigations:

- Investigations will be undertaken by the FMU. FMU may seek support from other relevant departments for investigations, as per requirement and the recommendations for action based on these investigations will include an element of risk assessment in conjunction with the Risk Management Function. The FMU shall report the status of significant cases of fraud detected in the Company to the FMC and to the Board of Directors on a quarterly basis through the RMC. FMU shall also maintain records of cases of frauds, as investigated by it, from those having intimated under Whistleblower Policy as well.
- The FMC is responsible for approving the final course of action on the fraud(s).
- Where an investigation shows involvement of employees of the Company, the Human Resource Department shall initiate appropriate process of action as recommended by the FMC

In other cases, suitable action shall be initiated by the FMU as recommended by the FMC.

6. REVIEW OF POLICY

The Anti-Fraud Policy shall be reviewed at least on an annual basis or such other shorter intervals as defined by the RMC and Board.

1. **Appendix A – List / Instances of Frauds/RFIs:**

Some of the examples of fraudulent acts/omissions include, but are not limited to the following:

A. Internal Fraud:

- misappropriating funds
- fraudulent financial reporting
- stealing /manipulating cheques
- overriding /decline decisions so as to bestow undue favour for family, friends & associates.
- inflating expenses/ claims / over billing
- paying false (or inflated) invoices, either prepared or obtained through collusion with suppliers.
- permitting special prices or privileges to customers, or granting business to favored suppliers, for kickbacks/favors.
- forging signatures
- removing money from customer accounts
- falsifying documents
- selling Company's assets at below their true value in return for payment.
- disclosing or selling confidential or proprietary information / documents to outside parties
- accepting or seeking anything of material value from contractors, vendors, or people providing services/materials to the Company

B. **Distribution Channel (Intermediary) Fraud:**

- Premium diversion - intermediary takes the premium from the purchaser and does not pass it to the Company.
- Inflates the premium, passing on the applicable amount to the Company and retaining the difference.
- Non-disclosure or misrepresentation of the risks to reduce premiums.
- Commission fraud – ensuring non-existent policyholders while paying a premium to the Company, collecting commission and annulling the insurance by ceasing further premium payments.

C. Policyholder Fraud and/or Claims Fraud

- Exaggerating damage / loss
- Staging the occurrence of incidents
- Reporting and claiming fictitious damage / loss
- Medical claims fraud
- Seeking insurance for non-existent assets
- Fraudulent actions in obtaining insurance coverage

D. External Fraud:

- Issue of fake policies of Company
- Acting in connivance with policyholders / prospects in obtaining fraudulent insurance coverage or raising fake claims or related manipulation
- Kickbacks/Bribes
- Shell companies
- Overcharging or fake billing to Company
- Inferior Goods
- Other frauds as may be classified by Company from time to time.

E. Cyber or New Age (Online) Fraud:

- Identity Theft
- Online Premium Siphoning (Payment Gateway & UPI Frauds)
- Forged / Fabricated policies
- Data theft / Breach
- Hacking of Company systems
- Malware attacks, Ransomware or intrusion into company digital infrastructure
- Phishing & Spoofing Fraud
- Impersonation