Fraud Risk Management Policy

1. INTRODUCTION

Medi Assist Insurance TPA Private Limited ('MAITPA' or 'the Company') as an IRDAI Licensed Third Party Administrator is committed to upholding ethical business conduct and compliance with the IRDAI (Insurance Fraud Monitoring Framework) Guidelines, 2025 ("Guidelines"). This policy establishes the internal standard operating framework to identify, prevent, detect, report and investigate insurance - related frauds.

2. SCOPE OF THE POLICY

Any activity with the intention of perpetuating fraud against the Company shall not be tolerated. The sole purpose of the policy is to keep on record and provide directions to the Company for prevention, detection, mitigation, reporting and remedy of fraud. This Policy is applicable to all Employees and Business Partners (as defined in this Policy).

3. OBJECTIVES OF THE POLICY

The policy inter alia intends:

1. A structured approach for identifying, assessing, and mitigating Fraud risks by setting clear standards for detection and prevention, implementing strong internal controls, and ensuring transparency in reporting and Investigations.
2. Clear responsibilities for assessing, managing and addressing Fraud risks.
3. Defined procedures, roles and accountability for managing and reporting Fraud cases.
4. Effective controls and mitigation strategies to support the prevention and early identification of fraudulent activities

4. DEFINITIONS

(i) **"Business Partners"** means any individual or organization that has commercial, contractual or professional relationship with the Company. This includes insurance intermediaries, such as agents, brokers and corporate agents, surveyors, loss assessors, investigators, panel advocates, service providers, consultants, vendors, outsourcing agencies, and any other party engaged in business transactions with the Company.

(ii) **"Cyber Fraud" or "New Age Fraud"** means any insurance fraud carried out using digital or new age technologies.

(iii) **"Governance Committee"** shall consist of the following officials:

1. Group Chief Financial Officer
2. Chief TPA Officer
3. President Claims
4. Company Secretary

(iv) **"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, suppressing or not disclosing one or more material facts relevant to any decision/ transaction, financial or otherwise, or
- Abusing responsibility, a position of trust or a fiduciary relationship.

(v) "Red Flag Indicator" ("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.

(vi) "Risk Management Committee" ("RMC") means a Committee constituted by the Board of Directors of the Company under the IRDAI Information and Cyber Security Guidelines 2026.

5. CLASSIFICATION OF FRAUD

Fraud may be broadly classified into the following categories:

(i) Internal Fraud: Fraud against the insurer, policyholders, customers or beneficiaries by internal staff, including Employees, senior management, or board members, either alone or in collusion with others, with an intent to defraud or deceive.

(ii) Distribution Channel Fraud: Fraud against the insurer, policyholders, customers or beneficiaries by Distribution Channels, either alone or in collusion with others, with an intent to defraud or deceive

(iii) 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, and includes but not limited to premium diversion, upcoding, unbundling services, billing for services never rendered

(iv) External Fraud: Fraud involving external parties' / service providers / vendors etc.

(v) Affinity Fraud or Complex Fraud: Fraud involving collusion among one or more Fraud perpetrators in the above categories.

(vi) Cyber or New Age Fraud: Fraud enabled or facilitated through digital channels or technology, including but not limited to business email compromise, phishing, synthetic identity creation, deepfakes, account takeover, unauthorised API access, and other technology-driven or new-age fraud typologies.

6. FRAUD RISK MANAGEMENT FRAMEWORK

The Company shall maintain a robust Fraud Risk Management Framework (FRMF) designed to proactively identify, assess, mitigate, and monitor fraud risks across all business functions. The Risk Management Committee (RMC) shall be responsible for effective implementation and oversight of

the fraud risk management framework. The framework is built upon the principle of Zero Tolerance toward fraud.

a. **Prevention and Control:** The Company will strive towards prevention of Fraud and shall have well defined procedures / measures of prevention techniques. In addition, the Company shall conduct the following activities:
   - Fraud detection through complaint data analysis.
   - Investigating the potential Fraud/Incident complaint, if any, received from time to time.
   - Identifying the control weakness and adopting the learnings for process enhancement.
   - Fraud risk assessment shall form part of the due diligence process for onboarding of new partners/vendors.
   - Establish and implement robust cybersecurity framework and monitoring in accordance with IRDAI Cyber Security Guidelines, 2026.
   - Establish communication channels and mechanisms, as outlined in this Policy and the Whistleblower Policy, to enable relevant stakeholders, including Employee and Business Partners, to report issues related to Fraud.
   - Periodic anti-fraud training for employees, network partners, and field investigation teams

b. **Detection and red flag indicators**: The Company utilizes automated claims management systems, and detects red flags including but not limited to:

- **Claims Red Flags:**
  - Multiple claims originating from the same hospital/doctor within short intervals with identical diagnoses.
  - Overlapping hospitalization dates for the same patient across different insurers.
  - High-value claims submitted right before policy expiry or right after policy inception.

- **Provider Red Flags:**
  - Sudden, disproportionate surge in cashless/reimbursement claim volumes from a specific hospital.
  - Universal usage of higher-end room categories or surgical procedures compared to regional baseline averages.

- **Internal & Employee Red Flags**
  - Frequent manual overrides of automated system checks, rule-engine rejections, or tariff caps by specific operational personnel.
  - Re-routing claim pay-outs or vendor disbursements to bank accounts sharing details (account numbers, PAN, IFSC) with internal employees or their close associates.

- **Policyholder / Claimant Red Flags**
  - Submission of hand-written, unnumbered, or non-letterhead bills, discharge summaries, or diagnostic reports containing typographical/formatting errors.
  - Mismatches in photo IDs, age, gender, or pre-existing condition declarations compared to historic medical or policy records.

- **Intermediary & Agent / Broker Red Flags**
  - Concentrated clusters of new policy issuances followed immediately by high-value, early claims managed through a specific agent/broker.
  - Multiple unrelated policyholders sharing identical email addresses, physical addresses, or mobile numbers linked back to an intermediary.

- **Digital & Cyber / IT Red Flags**
  - Cashless pre-authorization requests originating from IP addresses or geolocation points inconsistent with the treating hospital's physical location.
  - Repeated Failed Login / Portal Abuse.
  - Tampered uploads indicative of image modification, font manipulation, or erasure tool usage.

- The Company shall carry out a review of the Red Flag Indicators at a minimum of once in every 12 months.
- It is the duty of every employee of the company to provide information to the management which is within his/her knowledge about any fraud or potential fraud. This is not discretionary — it is a core obligation owed to the Company and its stakeholders.
- 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 overseeing office/department/ executive.
- **Reporting Channel:** All communication relating to suspected frauds must be immediately reported in writing to Governance Committee at fraudreporting@mediassist.in marked as “Confidential”.

  In case of letters, the fraud related communication should be sealed in an envelope marked “For the Attention of the Governance Committee” and must be handed over/sent to the Registered Office of the Company at the following address:

  To
  The Governance Committee
  Medi Assist Insurance TPA Private Limited
  Address: Tower "D", 4th Floor, IBC Knowledge Park, 4/1,
  Bannerghatta Road, Bengaluru-560 029
  Phone: +91 80 6919 0000

- The Company reserves the right to expand and establish additional reporting channels as deemed necessary to facilitate convenient and secure fraud related communication by all Stakeholders. Details of any new reporting mechanisms will be published and made accessible accordingly.

c. **Investigation and Reporting:**

Step 1: Preliminary Assessment (Days 1–5)

- Once a complaint is received the designated investigation team shall conduct a preliminary assessment within **5 business days** to determine if the report carries merit, sufficient detail, and falls within the scope of fraud.
- Members of the investigation team and/or the Governance Committee with potential conflicts of interest shall recuse themselves from the complaint.

Step 2: Formal Investigation & Evidence Gathering (Days 6–20)

- The designated investigation team shall immediately secure physical documents, emails, transaction logs, system records, and electronic devices (under strict chain of custody protocols to maintain legal admissibility).
- Fact-finding interviews shall be conducted with the Whistleblower/Complainant, witnesses, and the subject(s) under investigation. All interviews shall be formally documented and signed where applicable.

Step 3: Analysis, Findings & Final Reporting (Days 21–25)

- The investigation team will evaluate the gathered evidence to substantiate or refute the allegations, identify internal control gaps or collusion mechanisms.
- A detailed formal report will be compiled outlining the background, methodology, evidence, findings, financial impact, and key recommendations.
- The report shall be submitted to the Governance Committee for review and decision-making.

Step 4: Governance Action, Remediation & Recovery (Days 26–30)

- Based on the Committee's directions, appropriate action will be taken—ranging from employee termination, vendor blacklisting, and contract termination to filing police complaints (FIR) or initiating civil recovery proceedings.
- Operations teams shall implement corrective control measures within 30 days to remediate the identified vulnerabilities.
- Quarterly reports related to all Fraud complaints received is to be made Risk Management Committee.

d. **Fraud Monitoring**:

- The Company shall establish and maintain an "Incident Database" of relevant parties who have been convicted of Fraud or have attempted to defraud the insurer or Policyholder.
- The Company shall:
  i. assess the performance and trends of business generated through Distribution Channels.

ii. conduct regular audits focused on Fraud sensitivity to verify adherence to policies and procedures related to Insurance Fraud risk.
iii. continuously oversee vendor operations to ensure alignment with Fraud prevention strategies and contractual commitments.
iv. track customer complaints and grievances to identify and mitigate potential Fraud.
v. following the conclusion of every fraud investigation, the Company shall undertake a post-incident review to assess whether the Fraud could have been identified or prevented earlier, identify gaps in existing controls, and incorporate the learnings into the Fraud Risk Assessment, Red Flag Indicators and control environment on an ongoing basis.

7. CO-ORDINATION WITH LAW ENFORCEMENT AGENCIES

The Company and its employees shall co-operate with the law enforcement agencies for all the matters relating to this policy as mandated by the Guidelines.

8. WHISTLE BLOWER POLICY

Medi Assist Group has a well-defined "Whistle Blower Policy" which is applicable to and implemented fully by the Company.

9. CONFIDENTIALITY AND NON-RETALIATION

Under this Policy, the Company shall take reasonable efforts to protect the confidentiality of individuals who report suspected and/or actual Fraud. The identity of those providing information will be kept confidential to ensure investigations are conducted in a fair and thorough and appropriate manner. In a case where fraud is reported anonymously, the individual must provide credible and sufficient details to investigate effectively. The Company shall also ensure that no retaliatory action is taken against any person who, in good faith, reports known or suspected Fraud.

10. TRAINING, EDUCATION AND AWARENESS

To ensure effective implementation and promote a culture of transparency and accountability, periodic awareness sessions and formal training programs for all employees will be conducted. These initiatives will focus on educating employees on the existence, scope, and operational mechanics of this Policy, including the safeguards available against retaliation and the secure channels provided for reporting concerns in good faith.

11. REVIEW

This Policy shall be reviewed and approved by the Risk Management Committee and Board of Directors at least annually, or more frequently as mandated by applicable law or whenever the need arises, including on account of changes in the Company's risk profile, regulatory requirements or emerging Fraud trends.

Version Control:

Version	Creator/reviewer	Date of Board approval
1.0	Legal Department	August 06, 2026