



Anti-Fraud Policy

28-04-2026

This document is confidential and intended only for the internal use by Star Health and Allied Insurance Company Limited. The recipient(s) should ensure that this document is not reproduced or circulated to external entities in any form or means including electronic, mechanical, photocopying or otherwise without prior approval of the document owner or the primary recipients of this document. Should there be any conflict between the policy and the regulatory notifications, the latter shall prevail.

Key Policy Information:

Policy reference number	Policy Owner	Policy Approver	Creation date
SHAICL - Anti Fraud Policy	Chief Risk Officer	Board	23.03.2013

Summary - Version Control:

Version	Reviewed By	Approved By	Revision date	Reason for review
1.0	Chief Risk Officer	Board	FY 23	Periodic Review
2.0	Chief Risk Officer	Board	FY 24	Periodic Review
3.0	Chief Operating Officer	Board	FY 25	Changes on Ownership from CRO to COO, Change in Fraud addition of cyber related frauds and other minor changes.
4.0	Chief Operating Officer	Board	FY 26	Periodic Review
5.0	Chief Risk Officer	Board	FY 26	Change in ownership to CRO, changes done in alignment with Circular - IRDAI/IID/GDL/MISC/12/10/2025 dated 09-
5.0	Chief Risk Officer	Board	FY 27	Annual Review

Table of Contents

1. Introduction.....	3
1.1 Objective	3
1.2 Applicability / Scope.....	3
1.3 Review and Approval of the Policy	4
1.4 Zero Tolerance Policy.....	4
1.5 Fraud Risk Management by SHAIC.....	4
2 Policy Requirements.....	4
2.1 Definition & Introduction.....	4
2.2 Fraud Triangle	5
2.3 Illustrative List of Frauds	6
2.3.1 Internal Fraud	6
2.3.2 Policyholder Fraud and Claims Fraud.....	6
2.3.3 Distribution Channel Fraud	6
2.3.4 Cyber or New Age / Online frauds- Definition, meaning and understanding	7
2.3.5 External Frauds.....	7
2.3.6 Affinity/Complex Fraud	7
2.4 Roles and Responsibilities.....	8
2.4.1 Board of Directors	8
2.4.2 Board Risk Management Committee (BRMC).....	8
2.4.3 Fraud Monitoring Committee (FMC).....	8
2.4.4 Fraud Monitoring Unit (Vigilance / Fraud Control & Prevention Unit)	9
2.5 Preventive Mechanism	9
2.6 Procedure for Fraud Monitoring.....	10
2.7 Framework for Exchange of Information (In accordance with IRDAI guidelines)	10
2.8 Confidentiality.....	10
2.9 Identification and Reporting of Frauds	11
2.10 Whistleblower Protection	11
2.11 Co-ordination with Law Enforcement Agencies	11
2.12 Fraud Awareness.....	11
3 Reporting.....	11
4 Appendices	12
4.1 Related Policies and Procedures.....	12
4.2 List of applicable regulations	12
4.3 Summary of changes.....	12

1. Introduction

This Anti-Fraud Policy outlines the framework for preventing, detecting, investigating, and reporting fraud in compliance with IRDAI guidelines. Insurance fraud poses a significant threat to the integrity, financial stability, and trustworthiness of the insurance sector. In alignment with the Insurance Regulatory and Development Authority of India (IRDAI) Insurance Fraud Monitoring Framework Guidelines, 2025, this Anti-Fraud Policy establishes a comprehensive approach to deter, prevent, detect, report, and remedy fraud risks across all operations of the organization.

The policy aims to:

- Foster a culture of integrity and zero tolerance towards fraud.
- Protect the interests of policyholders and stakeholders.
- Ensure compliance with regulatory requirements and safeguard public trust.

Implement robust systems and processes for fraud risk management, including identification of red flag indicators, investigation protocols, and reporting mechanisms.

This policy applies to all employees, senior management, distribution channels, intermediaries, vendors, and any other stakeholders associated with the organization. It serves as a guiding framework for maintaining ethical standards and mitigating fraud risks effectively.

1.1 Objective

Effective deployment of controls which will aid in the identification, detection, prevention and investigations of frauds reported. SHAIC is dedicated to conducting business in a fair and honest manner and will work to eliminate fraud from all activities. SHAIC has a "Zero-Tolerance" stance to fraud and will not tolerate any dishonest or fraudulent behaviour on the part of internal or external stakeholders.

This policy covers the following aspects:

- Provide systems and adequate system-based controls to identify proactively potential fraud areas, assess these and provide a framework of people, process, and technology-based controls of processes to prevent fraud.
- Ensure that management understands the risk of fraud to the organization and establish a sound control environment through policies, procedures and controls to detect, monitor and mitigate occurrences of finds within various functions of SHAIC that are vulnerable to the fraud risk
- Create ongoing awareness among all stakeholders including employees, clients and other parties having business relation with SHAIC to deter them from indulging in fraudulent activities and measures to be taken by them in case they suspect any fraudulent activities.
- Provide a set of measures and procedures to respond adequately and quickly to frauds.
- Lay down procedures to report frauds to board, senior management and regulator and exchange of information on fraud and framework for reviewing the procedures from time to time

1.2 Applicability / Scope

This Policy applies to any fraud or suspected fraud involving employees as well as shareholders, consultants, vendors, contractors, outside agencies doing business with SHAIC and/or any other parties having a business

relationship with the SHAIC including insurance advisors/ brokers/ corporate agents of SHAIC. The policy would also be applicable to policyholders and beneficiaries. Any investigation activity required will be conducted irrespective of the suspected wrongdoer's length of service, position/title, or relationship to SHAIC.

All employees shall confirm to having read and understood this Policy and not violate any of its provision, on an annual basis, in the form as may be advised by the HR Department.

1.3 Review and Approval of the Policy

The Policy shall be reviewed annually by the Chief Risk Officer and approved by the Board. Fraud Monitoring Committee (FMC) shall assist the Board in the review process and recommend necessary changes in the policy. Policy may be reviewed by the Risk Management Team based on the newly released changes to Acts, regulatory requirements, independent audits and/or internal review.

1.4 Zero Tolerance Policy

SHAIC does not tolerate any unethical or dishonest behaviour, even if the result of the action benefits the SHAIC itself.

Any employee, intermediary, or vendor found guilty of fraud will face strict disciplinary action including termination and legal proceedings. Non-compliance with this policy will be treated as a serious breach and addressed as per the disciplinary matrix.

1.5 Fraud Risk Management by SHAIC

- i. SHAIC shall be constantly vigilant in deterring fraudsters. As part of their corporate governance the Board of SHAIC shall recognise and understand the risks of fraud to our organisation, including the potential types and impact of fraud. By understanding the risks of internal, external, policyholder, claims and distribution channel fraud, SHAIC shall decide which procedures and controls can be implemented effectively and efficiently to manage these risks.
- ii. SHAIC shall address fraud risk when establishing their mission, strategy and business objectives. The overall policy shall be consistently implemented in departmental objectives. It shall be reflected in the relevant operational procedures and controls.
- iii. For this purpose, SHAIC shall:
 - a. establish and maintain a sound control environment through policies, procedures and controls.
 - b. demonstrate a proper support by the Board and Senior Management ("tone at the top"), and overall communication of these values throughout their entire organisation.
 - c. organise and collect management information with respect to fraud in insurance, making it available in a timely manner for the Board and Senior Management to monitor developments and take appropriate action. This information shall be used to periodically evaluate the effectiveness of policies, procedures and controls and make changes where necessary.
- iv. As part of our fraud risk management, SHAIC shall have a set of measures and procedures to identify Red Flag Indicators (RFIs) to be able to respond adequately and quickly to (suspected) cases of fraud. These measures and procedures would include possible fraud investigation.

2 Policy Requirements

2.1 Definition & Introduction

"Fraud" in relation to affairs of a company or anybody corporate, includes 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;

“Wrongful gain” means the gain by unlawful means of property to which the person gaining is not legally entitled.

“Wrongful loss” means the loss by unlawful means of property to which the person losing is legally entitled.

Fraud in insurance is an act or omission intended to gain dishonest or unlawful advantage for a party committing the fraud or for other related parties. This may, for example, be achieved by means of:

- Misappropriating assets
- Deliberately misrepresenting, concealing, suppressing, or not disclosing one or more material facts relevant to the financial decision, transaction or perception of SHAIC’s status
- Abusing responsibility, a position of trust or a fiduciary relationship.

To adequately protect itself from the financial and reputational risks posed by insurance frauds, SHAIC shall have in place appropriate framework to detect, monitor, mitigate and report occurrence of such insurance frauds within SHAIC.

Financial Fraud poses a serious risk to all segments of the financial sector. Fraud in insurance reduces consumer and shareholder confidence; and can affect the reputation of SHAIC and the insurance sector as a whole. It also has the potential to impact economic stability. It is, therefore, required to understand the nature of fraud and take steps to minimize the vulnerability of operations to fraud.

2.2 Fraud Triangle

- i. There are three basic components that contribute to the occurrence of fraud, namely:

- motive/incentive
- opportunity
- rationalisation.

These basic components are often known as the fraud triangle.

- ii. People commit fraud for a variety of reasons. They could, for example, have financial problems or be under pressure to meet unrealistic business objectives. SHAIC shall be aware of the potential for these conditions to exist and look for signs of possible fraud.
- iii. Fraudsters need to have the opportunity to commit fraud. They are more likely to act when they think the likelihood of detection is small. Therefore, SHAIC shall have proper policies, procedures and controls to both prevent fraud from taking place and, if fraud does take place, to detect it.
- iv. Rationalisation is the mental process of justifying the fraud. For example, people may commit fraud because they:
 - are dissatisfied with an SHAIC as an employer
 - perceive an entitlement to compensation because of premiums paid
 - take an “everyone does it” attitude
 - are copying the behaviour of others in the SHAIC, such as the Board or Senior Management.

Also, public attitude regarding fraud in insurance does not deter fraud as many people see such fraud as a victimless crime.

2.3 Illustrative List of Frauds

Broadly, the potential areas of fraud include those committed by the officials of SHAIC, SHAIC's agent/corporate agent/intermediary/ and the policyholders/ their nominees. Some of the examples of fraudulent acts/omissions include, but are not limited to the following:

2.3.1 Internal Fraud

Fraud / misappropriation against SHAIC by its Director, Manager and/or any other officer or staff member (by whatever name called)

- i. Misappropriating funds
- ii. Fraudulent financial reporting
- iii. Overriding decline decisions so as to open accounts for family and friends
- iv. Inflating expenses claims/over billing
- v. Paying false (or inflated) invoices, either self-prepared or obtained through collusion with suppliers
- vi. Permitting special prices or privileges to customers, or granting business to favoured suppliers, for kickbacks/favours or misrepresentation of customer
- vii. Forging signatures
- viii. Removing money from customer accounts
- ix. Falsifying documents
- x. Selling SHAIC's assets at below their true value in return for payment.
- xi. Intentional concealment
- xii. Collusion or nexus with concerned stakeholders
- xiii. System Fraud

2.3.2 Policyholder Fraud and Claims Fraud

Fraud against the SHAIC in the purchase and/or execution of an insurance product, including fraud at the time of making a claim

- I. Exaggerating damages/loss
- II. Staging the occurrence of incidents
- III. Reporting and claiming of fictitious damage/loss
- IV. Medical claims fraud
- V. Fraudulent Death Claim
- VI. Non-Disclosure of Pre-Existing Disease (PED) illness before taking policy
- VII. Suppression of facts
- VIII. Duplicate or false claims

2.3.3 Distribution Channel Fraud

Fraud by Insurance Agents, Brokers, POSP, IMF, Corporate Agents

- I. Premium diversion-intermediary takes the premium from the purchaser and does not pass it to SHAIC
- II. Inflates the premium, passing on the correct amount to SHAIC and keeping the difference
- III. Non-disclosure or misrepresentation of the risk to reduce premiums
- IV. Commission fraud - ensuring non-existent policyholders while paying a first premium to SHAIC, collecting commission and annulling the insurance by ceasing further premium payments.
- V. Collusion or nexus with concerned stakeholders
- VI. Document Tampering, falsification of records and policy churning by the intermediaries to their advantage

The above list is illustrative and not exhaustive.

2.3.4 Cyber or New Age / Online frauds- Definition, meaning and understanding

Cyber / Online frauds refer to various kinds of frauds committed through internet, including phishing emails to gather personal data, hacking of servers/ computer systems, theft of data, password, cloning etc. Cyber / Online frauds can lead to:

- **Loss of Confidential Data:** Personally Identifiable Information (PII) collected and stored by the Company, including personal information of policyholders and, in some cases, of third parties.
- **Sensitive Information being compromised:** Star Health & Allied Insurance may collect sensitive business information and Physical Health Information (PHI) that could be valuable to corporate / foreign spies. In the case of certain lines such as cyber insurance products, the Company may possess information about a policyholder's network security controls and other cyber resilience information that could be valuable and could harm intellectual property rights of either party.
- **Disruption of Operations:** Cyber-attacks can result in disruption to normal business operation including emails, telephone directories, and voice mails amongst business records such as contract templates.
- **Loss of Trust:** If Star Health & Allied Insurance were to suffer a cyber-security incident that rendered it unable to make timely claims payments that trust may also be shaken. The reputational risk could extend to the sector as a whole.

The details of cyber frauds shall be read in conjunction with the information security policy.

2.3.5 External Frauds

Fraudulent acts committed by individuals or entities outside SHAIC, such as vendors, hospitals, diagnostic centres, service providers, and other third parties.

Vendor/Service Provider Fraud

- Submission of inflated or false invoices for services not rendered or partially rendered.
- Collusion with internal employees to approve fraudulent payments.
- Misrepresentation of credentials or capabilities during empanelment or contract execution.

Hospital/Healthcare Provider Fraud

- Overbilling for medical procedures or diagnostic tests.
- Charging for non-performed treatments or unnecessary procedures.
- Collusion with policyholders or intermediaries to generate fraudulent claims.

2.3.6 Affinity/Complex Fraud

Fraud involving collusion among multiple parties, often sophisticated in nature, aimed at causing financial or reputational harm to SHAIC. Examples include:

Organized Crime Rings

- Coordinated fraudulent claims targeting insurance products.
- Collusion between intermediaries, policyholders, and external entities to exploit loopholes in underwriting or claims processes.

Document-Based Fraud

- Use of forged or fabricated documents across multiple touchpoints to perpetrate fraud.
- Submission of falsified identity or medical records to support fraudulent claims.

Technology-Enabled Collusion

- Unauthorized access to SHAIC systems by external parties to manipulate data or transactions.
- Cyber-enabled collusion involving vendors and intermediaries to commit large-scale fraud.

2.4 Roles and Responsibilities

2.4.1 Board of Directors

The Board of Directors provide the overall guidance on fraud management and has delegated the responsibilities relating to fraud management activities to The Board Risk Management Committee (BRMC).

The Chief Risk Officer (CRO) independently reports to The Board Risk Management Committee. The Chief Risk Officer (CRO) is supported by the Vigilance, Internal Audit, Human Resource, Legal and Claims team for performing the fraud management activities of the organization.

Other functional heads shall also participate in responsibilities under the organization's anti-fraud strategy as they are directly responsible for overseeing areas of daily operations in which risk might arise as defined under the three lines of defence framework. Such function heads can serve as subject matter experts to assist the Chief Risk Officer with respect to their particular areas of expertise or responsibility.

2.4.2 Board Risk Management Committee (BRMC)

The Board Risk Management Committee (BRMC) is responsible for this policy and will remain, interpret and communicate the policy in the SHAIC. The committee is responsible for the following –:

- Effective implementation and oversight of fraud risk management framework.
- Monitor implementation of Anti-fraud policy for effective deterrence, prevention, detection and mitigation of frauds.
- The Board of Directors, senior leadership establish the "tone at the top" for ethical behaviour by acting ethically and expressing ethical requirements to employees honestly
- Review the issues identified during entity's fraud risk assessment as well as during internal and external audit
- The Board of Directors are informed on occurrence of any significant/material fraud incident through the quarterly reporting process.

2.4.3 Fraud Monitoring Committee (FMC)

Fraud Monitoring Committee shall be constituted consisting senior level officers headed by the CRO and CHRO being a part of FMC to ensure collaboration and appropriate reporting in the Board RMC.

The FMC is responsible for

- Review and monitoring of the Anti-Fraud policy.
- Operationalizing the Fraud risk management framework and oversee activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remediation
- Conduct an annual Comprehensive Fraud Risk Assessment to identify potential vulnerabilities across business lines.
- Develop mechanism to detect Red Flag Indicators (RFIs) in order to deter, prevent, detect, report, and mitigate fraud effectively across policy holder life cycle and also review the RFIs regularly for their continued relevance and effectiveness in detecting fraud.
- Design procedures for detecting, reporting, investigating and for taking proper action against the persons committing fraud

- Assess financial impact of frauds and submit the report to BRMC on quarterly basis.
- Initiate and oversee a prompt investigation of any suspected fraudulent act or omission or noncompliance with the policy's requirement.
- Ensure investigations are conducted & concluded within defined turnaround time (TAT).
- Ensure that this policy and related guidelines are communicated, updated and made available to all employees and representatives within the SHAIC
- Furnish reports on frauds to Authority, as required and an annual submission of the Fraud Monitoring Report (FMR) at the end of each financial year.
- Maintain an Incident Database of persons convicted of or attempting fraud.

2.4.4 Fraud Monitoring Unit (Vigilance / Fraud Control & Prevention Unit)

Fraud Monitoring Unit, Vigilance / Fraud Control & prevention Unit will be responsible for laying down appropriate fraud management processes and procedures in consultation with the CRO, across the Company and shall ensure effective implementation measures suggested by FMC. FMU shall report the status of significant cases of fraud detected in the Company to the Fraud Monitoring Committee (FMC) at least on a quarterly basis or earlier if required.

Functions of Fraud Monitoring Unit (Vigilance / Fraud Control & Prevention Unit) shall include but not be limited to the following:

Identify Potential areas of Fraud: Vigilance / Fraud Control & Prevention unit shall proactively try to identify potential areas of fraud. It shall undertake data analytics to find any fraud patterns/trends and subject the same to field/vigilance investigation. Further, it shall also analyse the data based on frauds detected during field/vigilance investigations.

- Vigilance / Fraud Control & Prevention unit shall collate all cases of frauds reported by the whistle-blower or any other entities.
- Vigilance / Fraud Control & Prevention unit shall investigate all such cases and render report to the duly highlighting the breaches of conduct, process and system etc. Report shall also highlight the financial implication, if any.

Disciplinary Action Process: For all proven cases, disciplinary action shall be initiated as per the defined disciplinary matrix and shall be shared with FMC for information. "Cases not covered under the Disciplinary Action Matrix shall be reviewed by the FMC for appropriate action."

Automation Initiatives: Active participation shall be taken by FMC in all automation initiatives related to proactive identification & mitigation of frauds.

Vigilance / Fraud Control & Prevention unit shall take appropriate steps to share information pertaining to fraud cases amongst all insurers, regulators, government authorities and to establish coordination platforms through the General Insurance Council/Insurance Information Bureau (IIB).

2.5 Preventive Mechanism

SHAIC shall inform both potential clients and existing clients about their fraud prevention policies. SHAIC shall take steps to appropriately include necessary caution in the insurance contracts / relevant

documents, duly highlighting the consequences of submitting a false statement and / or incomplete statement, for the benefit of the policyholders, claimants and the beneficiaries.

In addition, SHAIC shall conduct the following activities:

- Fraud Detection Through data analytics and document review
- Awareness on fraud among existing and prospective customers and identifying/reporting of suspicious activity.
- Investigate the whistle blower complaints, if any, received from time to time
- Establish a strong fraud risk & control assessment
- Regular and periodic training (including new-hire orientation and refresher training) shall be provided to all personnel, upon joining the organization and throughout their association with SHAIC, to clearly communicate expectations for ethical behaviour to staff members

2.6 Procedure for Fraud Monitoring

Vigilance / Fraud Control & Prevention unit & Internal Audit Department operating in the organizational set up will have the primary responsibility to identify, detect, and report insurance frauds.

SHAIC will have well defined procedures to identify, detect, investigate and report frauds. The risk management, fraud monitoring department and Information technology will develop/ manage systems and framework and analytical tool methodologies to identify potential fraud areas/ red flags.

For effective implementation of Fraud Risk Management Framework, SHAIC shall put in place appropriate measures to identify and assess fraud risks and shall track business trends from distribution channels, continuously monitoring vendor activities for compliance with fraud prevention measures and contractual obligations, and analysing customer grievances and complaints to detect and prevent fraud.

2.7 Framework for Exchange of Information (In accordance with IRDAI guidelines)

In accordance with the IRDAI guidelines and industry best practices, the SHAIC shall actively participate in the **Insurance Information Bureau of India (IIB) Fraud Monitoring Framework** to strengthen fraud prevention and detection measures.

Key Commitments:

- Mandatory Participation**
The organization will integrate with IIB's fraud monitoring technology platform to share and access industry-wide fraud intelligence.
- Data Sharing & Threat Intelligence**
Share information on blacklisted entities, including distribution channels, hospitals, vendors, and individuals
- Compliance Monitoring**
Regularly review adherence to IIB timelines and procedures and maintain audit trails for all submissions.

2.8 Confidentiality

All fraud investigation and related information will be treated confidentially. Investigation results will not be disclosed or discussed with anyone other than those who have a valid business need to know. This is important to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct.

2.9 Identification & Reporting of Frauds

SHAIC strongly All persons including employees, vendors, , agents, intermediaries are expected to take all reasonable steps to prevent the occurrence of Frauds including online Frauds and to identify and report instances of known or suspicious Fraud committed against the Company, whether by the employees or by outside parties. Complaints/disclosures shall be dwelt in accordance with the Whistle-blower Policy (whistleblower@starhealth.in).

2.10 Whistleblower Protection

SHAIC strongly encourages individual to report fraudulent activity. Any employee of SHAIC making a report in good faith, can do so in the knowledge and confidence that the Board of Directors / senior management of SHAIC will ensure that the act will not lead to the employee facing any recrimination, punishment or victimization.

SHAIC is committed to fostering a culture of transparency and integrity. To support this, the organization has established a robust whistleblower mechanism that ensures employees and stakeholders can report suspected fraudulent activities without fear of retaliation.

2.11 Co-ordination with Law Enforcement Agencies

Whenever an allegation of fraud of grave nature is prima facie found to be true, efforts will be taken to file a complaint with police authorizes for initiating action under criminal law of the land. The Vigilance and Legal departments will help in drafting the complaints and in liaison with the Police

2.12 Fraud Awareness

Training can help to raise staff awareness of the risk of fraud and the importance of compliance with internal control procedures and security checks to prevent such frauds additionally, close monitoring of staff / intermediary compliance with these controls helps ensure their consistent application. The management shall consider developing fraud awareness initiatives that are

- Comprehensive and based upon job functions and risk areas
- Integrated with other training efforts, whenever possible
- Regular and frequent, covering the relevant employee / intermediaries' population

There shall be communication to both potential and existing clients about SHAIC's anti-fraud policies.

Risk management team will share awareness communications on periodic basis with motive to spread awareness among employees at all levels about new emerging risks, insurance frauds and ways of preventing fraud.

3 Reporting

SHAIC shall furnish the statistics on various fraudulent cases which come to light and action taken thereon shall be filed with the Authority in forms FMR 1 providing details of

- Outstanding fraud cases; and
- Closed fraud cases

Within 30 days of the close of every financial year.

Fraud committed by distribution channels registered by IRDAI, shall be immediately reported to IRDA

4 Appendices

4.1 Related Policies and Procedures

This policy shall be read in conjunction with the following Policies and Procedures:

- Anti-Money Laundering Policy
- Whistle-blower Policy
- Enterprise Risk Management (ERM) Policy
- Disciplinary Action matrix
- Service rules

4.2 List of applicable regulations

Date of issuance	Ref. No	Name of Legislation
02-04-2002	F. No. IRDA/REG/03/2002	IRDAI (Preparation of Financial Statements and Auditors Report of Insurance Companies) Regulations, 2002
21-01-2013	No. IRDA/SDD/MISC/CIR/009/01/2013	Insurance Fraud Monitoring Framework
18-05-2016	IRDA/F&A/GDL/CG/100/05/2016	Corporate Governance Guidelines for Insurance Companies
09-03-2017	IRDA/INT/GDL/ECM/055/03/2017	Guidelines on Insurance e-commerce
09-10-2025	IRDAI/IID/GDL/MISC/112/10/2025	Insurance Regulatory and Development Authority of India (Insurance Fraud Monitoring Framework) Guidelines, 2025 effective from 1 Apr 2026.

4.3 Summary of changes

Version	Page No.	Section	Summary of Key Changes in the Policy
5	1	NA	Policy ownership changed to Chief Risk Officer(CRO)
5	6	2.3	Two new categories of fraud; external fraud & affinity fraud introduced under the “Illustrative List of Frauds” section.
5	8	2.4.3	Renaming Fraud Risk Mitigation Committee(FRMC) as Fraud Monitoring Committee(FMC) and aligning roles & responsibility as per IRDAI guidelines
5	8	2.4.3	Annual Fraud Risk Assessment included as the key responsibility of FMC
5	8	2.4.3	Developing mechanism to detect Red Flag Indicators(RFIs) during the entire policy holder life cycle included under the responsibilities of FMC
5	8	2.4.3	Assessment of financial impact of frauds included under the responsibilities of FMC
5	10	2.7	Framework of Exchange of Information with IIB updated as per IRDAI guidelines

Detailed Summary of Changes in Anti-Fraud Policy-FY26

Version	Page No.	Section	Erstwhile Section	New/Modified Section
5	1	NA	Policy Owner Chief Operating Officer	Policy Owner Chief Risk Officer
5	3	1	Introduction Addition	Introduction This Anti-Fraud Policy outlines the framework for preventing, detecting, investigating, and reporting fraud in compliance with IRDAI guidelines. Insurance fraud poses a significant threat to the integrity, financial stability, and trustworthiness of the insurance sector. In alignment with the Insurance Regulatory and Development Authority of India (IRDAI) Insurance Fraud Monitoring Framework Guidelines, 2025, this Anti-Fraud Policy establishes a comprehensive approach to deter, prevent, detect, report, and remedy fraud risks across all operations of the organization. The policy aims to: - Foster a culture of integrity and zero tolerance towards fraud. - Protect the interests of policyholders and stakeholders. - Ensure compliance with regulatory requirements and safeguard public trust. Implement robust systems and processes for fraud risk management, including identification of red flag indicators, investigation protocols, and reporting mechanisms. This policy applies to all employees, senior management, distribution channels, intermediaries, vendors, and any other stakeholders associated with the organization. It serves as a guiding framework for maintaining ethical standards and mitigating fraud risks effectively.
5	4	1.1	Background In accordance with the Insurance Fraud Monitoring Framework, dated January 21, 2013 (hereinafter referred to as “the Framework”), SHAIC is required to have in place an Anti-Fraud Policy (hereinafter referred to as “the Policy”), duly approved by the Board of Directors. Further, as laid down in the “Guidelines on Insurance e-commerce” dated March 9, 2017, an Insurer is required to have a pro-active fraud detection policy for insurance e-commerce activities, which is to be approved by the Board of Directors. Also, Corporate Governance Guidelines for Insurance Companies dated May 18, 2016 issued by IRDAI, requires insurance companies for formulation of a Fraud monitoring policy and framework for effective deterrence, prevention, detection and mitigation of frauds.	Background Deletion

			This Policy has been further devised to ensure that the fraud detection framework is in line with the requirements as laid down under the Framework, as well as it recognizes the principle of proportionality and reflects the nature, scale and complexity of the business of the Company and risks to which it is exposed. The Policy shall also provide guidance with respect to prevention, detection, mitigation and investigation into fraudulent activities. In order to provide regulatory supervision and guidance on the adequacy of measures taken by insurers to address and manage risk emanating from fraud, the IRDA vide its circular no. IRDA/SDD/MISC/CIR/009/01/2013 dated January 21, 2013 (Circular) laid down the guidelines requiring insurance companies to have in place the Fraud Monitoring Framework. The circular mandates all insurance companies to put in place, as part of their corporate governance structure, a Fraud Monitoring Framework. Further, to address and manage risks emanating specifically from online e-commerce fraud, IRDAI vide its circular No. IRDA/INT/GDL/ECM/055/03/2017 dated March 9, 2017 laid down the guidelines requiring insurance companies to include Insurance e-commerce in their Fraud Monitoring Framework. The Circular mandates the insurers to have a pro-active fraud detection policy for the insurance e-commerce.	
5	5	1.4	Review and approval of the policy This policy shall be reviewed and approved annually by the Board. Fraud Risk Mitigation Committee (FRMC) shall assist the Board in the review process and recommend necessary changes in the policy. Policy may be reviewed by the Fraud Control & Prevention department (FCP) based on the newly released changes to Acts, regulatory requirements, independent audits and/ or internal review	Review and approval of the policy The Policy shall be reviewed annually by the Chief Risk Officer and approved by the Board. Fraud Monitoring Committee (FMC) shall assist the Board in the review process and recommend necessary changes in the policy. Policy may be reviewed by the Risk Management Team based on the newly released changes to Acts, regulatory requirements, independent audits and/or internal review.
5	4	1.4	Zero Tolerance Policy Action as deemed fit will be initiated including termination and referring the case to appropriate government authorities.	Zero Tolerance Policy Any employee, intermediary, or vendor found guilty of fraud will face strict disciplinary action including termination and legal proceedings. Non-compliance with this policy will be treated as a serious breach and addressed as per the disciplinary matrix

5	4	1.5	Introduction New Addition	Introduction Fraud risk management by SHAIC i) SHAIC shall be constantly vigilant in deterring fraudsters. As part of their corporate governance the Board of SHAIC shall recognise and understand the risks of fraud to our organisation, including the potential types and impact of fraud. By understanding the risks of internal, external, policyholder, claims and distribution channel fraud, SHAIC shall decide which procedures and controls can be implemented effectively and efficiently to manage these risks. ii) SHAIC shall be address fraud risk when establishing their mission, strategy and business objectives. The overall policy shall be consistently implemented in departmental objectives. It shall be reflected in the relevant operational procedures and controls. iii) For this purpose, it is essential that an SHAIC shall: a) establish and maintain a sound control environment through policies, procedures and controls. b) demonstrate a proper support by the Board and Senior Management (“tone at the top”), and overall communication of these values throughout their entire organisation. c) organise and collect management information with respect to fraud in insurance, making it available in a timely manner for the Board and Senior Management to monitor developments and take appropriate action. This information shall be used to periodically evaluate the effectiveness of policies, procedures and controls and make changes where necessary. iv) As part of our fraud risk management, SHAIC shall have a set of measures and procedures to identify Red Flag Indicators (RFIs) to be able to respond adequately and quickly to (suspected) cases of fraud. These measures and procedures would include possible fraud investigation.
5	5	2.1	Policy Requirements Definition & Introduction In order to adequately protect itself from the financial and reputational risks posed by insurance frauds, SHAIC shall have in place appropriate framework to detect, monitor, mitigate and report occurrence of such insurance frauds within SHAIC.	Policy Requirements Definition & Introduction To adequately protect itself from the financial and reputational risks posed by insurance frauds, SHAIC shall have in place appropriate framework to detect, monitor, mitigate and report occurrence of such insurance frauds within SHAIC.
5	5	2.2	Policy Requirements Fraud Triangle Addition	Policy Requirements Fraud Triangle i. There are three basic components that contribute to the occurrence of fraud, namely: • motive/incentive • opportunity • rationalisation.

				These basic components are often known as the fraud triangle. ii. People commit fraud for a variety of reasons. They could, for example, have financial problems or be under pressure to meet unrealistic business objectives. SHAIC shall be aware of the potential for these conditions to exist and look for signs of possible fraud. iii. Fraudsters need to have the opportunity to commit fraud. They are more likely to act when they think the likelihood of detection is small. Therefore, SHAIC shall have proper policies, procedures and controls to both prevent fraud from taking place and, if fraud does take place, to detect it. iv. Rationalisation is the mental process of justifying the fraud. For example, people may commit fraud because they: • are dissatisfied with an SHAIC as an employer • perceive an entitlement to compensation because of premiums paid • take an “everyone does it” attitude • are copying the behaviour of others in the SHAIC, such as the Board or Senior Management. Also, public attitude regarding fraud in insurance does not deter fraud as many people see such fraud as a victimless crime.
5	6	2.3.2	Illustrative List of Frauds Policyholder Fraud and Claims Fraud: Examples of some other important types of frauds: ▪ Vendor fraud (e.g., Kickbacks including the receipt of excessive gifts or accepting or seeking anything of material value from contractors, vendors or persons providing services/materials); ▪ Forgery or alteration of documents or accounts belonging to the Company; of transactions, assets or liabilities; Concealment or misrepresentation ▪ Expense report fraud (e.g., claims for services or goods not actually provided, seeking fake reimbursements); ▪ Loss of intellectual property (e.g., disclosing confidential and proprietary information to outside parties); ▪ Conflicts of Interest resulting in actual or exposure to financial loss; ▪ Embezzlement (e.g. misappropriation of money, securities, supplies, property or other assets); ▪ Cheque	Illustrative List of Frauds Policyholder Fraud and Claims Fraud: Deletion

			fraud (forgery or alteration of cheques, bank drafts or any other financial instrument); ▪ Payroll fraud; ▪ Bribery & corruption (misusing the vested authority to seek personal gains); ▪ Fraudulent financial reporting (e.g. forging or alteration of accounting documents or records; intentional concealment or misstatement of transactions resulting in falsification of records or misleading statements; ▪ Intentional failure to record or disclose significant information accurately or completely ▪ Improper pricing activity; ▪ Unauthorized or illegal use of confidential information (e.g. profiteering as a result of insider knowledge of company activities); ▪ Electronic Fraud and/or illegal hacking, unauthorized or illegal manipulation of information technology networks or operating systems; ▪ Tax evasion; ▪ Destruction, removal or inappropriate use of records, furniture, fixtures and equipment of the Company; Sales or assignment of fictitious or misrepresented assets; ▪ Utilizing company funds for personal purposes.	
5	6	2.3.3	Intermediary Fraud To protect its e-commerce business, the company will also oversee the adoption of proactive fraud detection measures in conjecture with IRDAI Guidelines on insurance e-commerce (IRDA/tTNT/ GDU ECM/ 055t O3t 2017) Dtd. 9th March 2017.	Distribution Channel Fraud Deletion
5	7	2.3.4	Cyber / Online frauds- Definition, meaning and understanding: Sensitive Information being compromised: Star Health & Allied Insurance may collect sensitive business information that could be valuable to corporate / foreign spies. In the case of certain lines such as cyber insurance products, the Company may possess information about a policyholder's network	Cyber or New Age / Online frauds- Definition, meaning and understanding: • Sensitive Information being compromised: Star Health & Allied Insurance may collect sensitive business information and Physical Health Information (PHI) that could be valuable to corporate / foreign spies. In the case of certain lines such as cyber insurance products, the Company may possess information about a policyholder's network security controls and other cyber resilience

			security controls and other cyber resilience information that could be valuable and could harm intellectual property rights of either party. Cyber frauds should be reported to cybersecurity.helpdesk@starhealth.in.	information that could be valuable and could harm intellectual property rights of either party. Deletion
5	7	2.3.5 & 2.3.6	Illustrative List of Frauds Addition	Illustrative List of Frauds External Frauds - Fraudulent acts committed by individuals or entities outside SHAIC, such as vendors, hospitals, diagnostic centres, service providers, and other third parties. Vendor/Service Provider Fraud •Submission of inflated or false invoices for services not rendered or partially rendered. •Collusion with internal employees to approve fraudulent payments. •Misrepresentation of credentials or capabilities during empanelment or contract execution. Hospital/Healthcare Provider Fraud •Overbilling for medical procedures or diagnostic tests. •Charging for non-performed treatments or unnecessary procedures. •Collusion with policyholders or intermediaries to generate fraudulent claims. f. Affinity/Complex Fraud – Fraud involving collusion among multiple parties, often sophisticated in nature, aimed at causing financial or reputational harm to SHAIC. Examples include: Organized Crime Rings •Coordinated fraudulent claims targeting insurance products. •Collusion between intermediaries, policyholders, and external entities to exploit loopholes in underwriting or claims processes. Document-Based Fraud •Use of forged or fabricated documents across multiple touchpoints to perpetrate fraud. •Submission of falsified identity or medical records to support fraudulent claims. Technology-Enabled Collusion •Unauthorized access to SHAIC systems by external parties to manipulate data or transactions. •Cyber-enabled collusion involving vendors and intermediaries to commit large-scale fraud.

5	10	2.3.1	Roles and Responsibilities Board of Directors The Board of Directors provide the overall guidance on fraud management and has delegated the responsibilities relating to fraud management activities to the Board Risk Management Committee (BRMC). The Chief Human Resources Officer (CHRO) independently reports to the board risk management committee. The Chief Human Resources Officer (CHRO) is supported by the risk, investigation, Vigilance, Internal Audit, underwriting and claims team for performing the fraud management activities of the organization. Other business leaders such as functional heads should also participate in responsibilities under the organization's anti fraud strategy as they are directly responsible for overseeing areas of daily operations in which risk might arise as defined under the three lines of defence framework. Such function heads can serve as subject matter experts to assist the Chief Operating Officer with respect to their particular areas of expertise or responsibility.	Roles and Responsibilities Board of Directors The Board of Directors provide the overall guidance on fraud management and has delegated the responsibilities relating to fraud management activities to The Board Risk Management Committee (BRMC). The Chief Risk Officer (CRO) independently reports to The Board Risk Management Committee. The Chief Risk Officer (CRO) is supported by the Vigilance, Internal Audit, Human Resource, Legal and Claims team for performing the fraud management activities of the organization. Other functional heads shall also participate in responsibilities under the organization's anti-fraud strategy as they are directly responsible for overseeing areas of daily operations in which risk might arise as defined under the three lines of defence framework. Such function heads can serve as subject matter experts to assist the Chief Risk Officer with respect to their particular areas of expertise or responsibility.
5	8	2.4.2	Roles and Responsibilities Board Risk Management Committee (BRMC) Addition To ensure the Board of Directors are informed on occurrence of any fraud incident through quarterly reporting process.	Roles and Responsibilities Board Risk Management Committee (BRMC) Effective implementation and oversight of fraud risk management framework. The Board of Directors are informed on occurrence of any significant/material fraud incident through the quarterly reporting process.
5	8-9	2.4.3	Roles and Responsibilities Fraud Risk Mitigation Committee (FRMC) Fraud Risk Mitigation Committee (FMRC) shall be constituted consisting of three senior level officers not below the rank of GMs headed by the CHRO and CRO being a part of FRMC in order to ensure collaboration and appropriate reporting in the Board RMC. The quorum shall	Roles and Responsibilities Fraud Monitoring Committee (FMC) Fraud Monitoring Committee shall be constituted consisting senior level officers headed by the CRO and CHRO being a part of FMC in order to ensure collaboration and appropriate reporting in the Board RMC.

			be 2 committee members with CHRO and Head of Fraud Control and Prevention being the convenor of the committee. The FRMC is responsible • Creation and review of the Anti-Fraud policy. • To design procedures for detecting, reporting, investigating and for taking proper action against the persons committing fraud • Create awareness among employees, intermediaries, and policyholders to counter insurance frauds • To initiate and oversee a prompt investigation of any suspected fraudulent act or omission or noncompliance with the policy's requirement • To ensure that this policy and related guidelines are communicated, updated and made available to all employees and representatives within the SHAIC • For recovery of loss from the persons committing fraud against the SHAIC • To ensure that Board of Directors are informed of fraud on occurrence of any fraud incident through periodical reporting process • Furnish reports on frauds to Authority, as required and an annual submission of the Fraud Monitoring Report (FMR) at the end of each financial year. • Coordinate with the Internal Audit and Vigilance mechanism in SHAIC to report to the Risk Management Committee and the Board.	The FMC is responsible for • Review and monitoring of the Anti-Fraud policy. • Operationalizing the Fraud risk management framework and oversee activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remediation • Conduct an annual Comprehensive Fraud Risk Assessment to identify potential vulnerabilities across business lines. • Review Red Flag Indicators (RFIs) to proactively identify frauds during entire policy holder life cycle and also review the RFIs regularly for their continued relevance and effectiveness in detecting fraud. • Design procedures for detecting, reporting, investigating and for taking proper action against the persons committing fraud • Assess financial impact of frauds and submit the report to BRMC on quarterly basis. • Initiate and oversee a prompt investigation of any suspected fraudulent act or omission or noncompliance with the policy's requirement. • Ensure investigations are conducted & concluded within defined turnaround time (TAT). • Ensure that this policy and related guidelines are communicated, updated and made available to all employees and representatives within the SHAIC • Furnish reports on frauds to Authority, as required and an annual submission of the Fraud Monitoring Report (FMR) at the end of each financial year. • Maintain an Incident Database of persons convicted of or attempting fraud.
5	9-10	2.4.4	Roles and Responsibilities Fraud Control & Prevention Unit / Vigilance Fraud Control & prevention Unit / Vigilance will be responsible for laying down appropriate fraud management processes and procedures in consultation with the CHRO, across the Company. It shall report the status of significant cases of fraud detected in	Roles and Responsibilities Fraud Monitoring Unit (Vigilance / Fraud Control & Prevention Unit). Fraud Monitoring Unit, Vigilance / Fraud Control & prevention Unit will be responsible for laying down appropriate fraud management processes and procedures in consultation with the CRO, across the Company and shall ensure effective implementation measures suggested by FMC. FMC shall report the status of significant cases

		the Company to the Fraud Risk Mitigation Committee (FRMC) headed by the CHRO at least on a quarterly basis or earlier if required. <u>Functions of Fraud Control & Prevention Unit / Vigilance shall include but not be limited to the following:</u> Identify Potential areas of Fraud: Fraud Control & Prevention unit / Vigilance shall proactively try to identify potential areas of fraud. It shall undertake data analytics to find any fraud patterns/trends and subject the same to field/vigilance investigation. Further, it shall also analyse the data based on frauds detected during field/vigilance investigations. -Fraud Control & Prevention Unit / Vigilance shall collate all cases of frauds reported by the whistle-blower or any other entities. · -Fraud Control & Prevention unit / Vigilance shall investigate all such cases and render report to the duly highlighting the breaches of conduct, process and system etc. Report shall also highlight the financial implication, if any. -Fraud Control & Prevention unit / Vigilance shall get the cases having involvement of non-related entities reviewed and closed through Head –Fraud control Unit / CVIO and submit details of such cases to the FRMC. Disciplinary Action Process: For all proven cases, disciplinary action should be initiated as per the defined disciplinary matrix/ service rules and should be shared with FRMC for information. Automation Initiatives: Active participation should be taken by FRMC & Fraud Control & Prevention Unit in all automation initiatives related to proactive identification & mitigation of frauds. Fraud Control & Prevention Unit / Vigilance shall take appropriate steps to share	of fraud detected in the Company to the Fraud Monitoring Committee (FMC) at least on a quarterly basis or earlier if required. <u>Functions of Fraud Monitoring Unit (Vigilance / Fraud Control & Prevention Unit) shall include but not be limited to the following:</u> Identify Potential areas of Fraud: Vigilance / Fraud Control & Prevention unit shall proactively try to identify potential areas of fraud. It shall undertake data analytics to find any fraud patterns/trends and subject the same to field/vigilance investigation. Further, it shall also analyse the data based on frauds detected during field/vigilance investigations. • Vigilance / Fraud Control & Prevention unit shall collate all cases of frauds reported by the whistle-blower or any other entities. · • Vigilance / Fraud Control & Prevention unit shall investigate all such cases and render report to the duly highlighting the breaches of conduct, process and system etc. Report shall also highlight the financial implication, if any. · Disciplinary Action Process: For all proven cases, disciplinary action shall be initiated as per the defined disciplinary matrix and shall be shared with FMC for information. “Cases not covered under the Disciplinary Action Matrix shall be reviewed by the FMC for appropriate action.” Automation Initiatives: Active participation shall be taken by FMC in all automation initiatives related to proactive identification & mitigation of frauds. Vigilance / Fraud Control & Prevention unit shall take appropriate steps to share information pertaining to fraud cases amongst all insurers, regulators, government authorities and to establish coordination platforms through the General Insurance Council/Insurance Information Bureau (IIB).
--	--	--	---

			information pertaining to fraud cases amongst all insurers, regulators, government authorities and to establish coordination platforms through the General Insurance Council/Insurance Information Bureau (IIB).	
5	9	NA	Roles and Responsibilities Nodal Officer a. Appointment of Nodal Officer In corporate office there shall be a Nodal officer not the below rank of GM who will act as overall coordinator of the entire organization. -Competent Authority concerned will notify the name and designation of link Nodal Officer who will discharge the duties and responsibilities of nodal officer during his/her leave. b. Responsibility Nodal Officer shall share the responsibility of prevention and detection of fraud and for implementing the "Anti-Fraud Policy" of the SHAIC. It is the responsibility of all Nodal Officer to ensure that complete mechanism in respect of Fraud Prevention Policy is in place within his/her area of control to: -Familiarise each employee with the measures to be taken for prevention and detection of fraud. -Create a whistleblowing culture whereby employees are encouraged to report any fraud or suspected fraud which comes to their knowledge, without any fear of victimization. Promote awareness among the employees of ethical standards. -Creating awareness among employees / intermediaries / policy holders to counter insurance frauds. -Coordinating with the Fraud control & Prevention Unit / Vigilance Dept. to	Roles and Responsibilities Nodal Officer Deletion

			investigate the complaints of fraud and secure necessary documentary evidence -Liaise with Human Resource Management, marketing, claims Department to take disciplinary action against employees / intermediary under Conduct, Discipline and Appeal (CDA) Rules if they are found to have been involved -Furnishing various reports on frauds to the Authority as stipulated in this regard and Furnish periodic reports to the Board for its review. -The Nodal Officer shall implement the modules suggested by the FRMC to create awareness among the employees and officers in fraud detection and mitigation.	
5	9	NA	Roles and Responsibilities Employees Employees and officers at every level, in every function, at all offices of SHAIC and at all the locations have a responsibility to speak up when they believe that they have knowledge or suspect that fraud is being committed. As soon as it is learnt that a fraud or suspected fraud has taken or is likely to take place, they should immediately apprise the same to the concerned party as per the laid down whistleblowing policy in place.	Roles and Responsibilities Employees Deletion
5	9	NA	Roles and Responsibilities Code of Conduct An organization's code of conduct is one of the most important communications that anagement should use to communicate to employees on key standards that define acceptable business conduct. The code of conduct should be in place based on below key attributes: -High-level endorsement from the organization's leadership, underscoring a commitment to integrity -Simple, concise and positive language that can be readily understood by employees	Roles and Responsibilities Code of Conduct Deletion

			-Guidelines on each of the SHAIC's major policies or compliance risk areas • Ethical decision-making tools to assist employees in making right choices -A designation of reporting channels and viable mechanisms that employee can use to report concerns or seek advice without fear of retaliation	
5	9-10	2.5	Preventive Mechanism SHAIC shall put up a notice board in every office mentioning the name of the Nodal Officer, phone No. and Official address to enable every person to send intimation about commission of Fraud or suspected Fraud.	Preventive Mechanism In addition, SHAIC shall conduct the following activities:
5	10	2.6	Procedure for Fraud Monitoring Internal Audit, Fraud Control & Prevention unit and Vigilance Department operating in the organizational set up will have the primary responsibility to identify, detect, and report insurance frauds. While the Audit and Fraud Control & Prevention unit will monitor fraudulent activities during their exercise, the Vigilance Department will carry out the exercise during their surprise inspection of offices from time to time. SHAIC will have well defined procedures to identify, detect, investigate and report frauds. The risk management, fraud monitoring department and Information technology will develop/ manage systems and framework and analytical tool methodologies to identify potential fraud areas/ red flags.	Procedure for Fraud Monitoring Vigilance / Fraud Control & Prevention unit & Internal Audit Department operating in the organizational set up will have the primary responsibility to identify, detect, and report insurance frauds. SHAIC will have well defined procedures to identify, detect, investigate and report frauds. The risk management, fraud monitoring department and Information technology will develop/ manage systems and framework and analytical tool methodologies to identify potential fraud areas/ red flags. For effective implementation of Fraud Risk Management Framework, SHAIC shall put in place appropriate measures to identify and assess fraud risks and shall track business trends from distribution channels, continuously monitoring vendor activities for compliance with fraud prevention measures and contractual obligations, and analysing customer grievances and complaints to detect and prevent fraud.
5	10	NA	Identification and reporting of frauds All persons including employees, vendors, TPAs, agents, intermediaries are expected to take all reasonable steps to prevent the occurrence of Frauds including online Frauds and to identify and report instances of known or suspicious Fraud committed against the Company, whether by the employees or by outside parties. Fraud should be timely,	Identification and reporting of frauds Deletion

			expeditiously, unhesitatingly and fearlessly report any Fraud including Online Fraud, against the Company to the Fraud Control at fraudmitigation@starhealth.in . Complaints/disclosures made against or in relation to employees of the Company shall be dwelt in accordance with the Whistle-blower Policy (whistleblower@starhealth.in) and complaints/disclosures against any person / entity other than employees of the Company shall be dwelt in accordance with the provisions of this Policy. No employee shall investigate / interview / interrogate such cases of actual / suspected frauds himself except responsible person within Fraud Control Fraud Control and Prevention and Vigilance function shall ensure that the internal reporting mechanism shall be made known and available to all the employees and third parties such as customers, vendors and other third parties who conduct business with SHAIC through reference in SHAIC's website and other external communication materials.	
5	10	2.7	Framework for exchange of information Framework for exchange of information (In accordance with IRDAI guidelines) In accordance with the IRDAI guidelines and industry best practices, the SHAIC shall actively participate in the Insurance Information Bureau of India (IIB) Fraud Monitoring Framework to strengthen fraud prevention and detection measures. Key Commitments: i) Mandatory Participation The organization will integrate with IIB's fraud monitoring technology platform to share and access industry-wide fraud intelligence relevant to our business operations. ii) Data Sharing & Threat Intelligence Share information on blacklisted entities, including distribution channels, hospitals, vendors, and individuals iii) Compliance Monitoring Regularly review adherence to IIB reporting timelines and procedures and maintain audit trails for all submissions.	

5	10	NA	Due Diligence SHAIC will ensure that pre-employment verification is done for all employees in the cadre of AGM and above (Non marketing) and for ABM and above (Marketing) steps will be taken to ascertain the antecedents of insurance agent/corporate agent/intermediary/TPAs before appointment/agreements with them.	Due Diligence Deletion
5	10	NA	Regular Communication Channels Risk Management, Fraud Monitoring Unit, HR, Vigilance, any other function who is involved in identification of a fraud to generate fraud mitigation communication within SHAIC at periodic intervals or on ADHOC basis, as may be required. It must also ensure information flow to concerned departments with respect to frauds.	Regular Communication Channels Deletion
5	11	2.9	Security to Individuals However, any abuse of this protection (e.g. any false or bogus allegation made by an individual knowing them to be false or bogus or with a mala fide intention) will warrant action as deemed necessary by SHAIC.	Whistleblower Protection SHAIC is committed to fostering a culture of transparency and integrity. To support this, the organization has established a robust whistleblower mechanism that ensures employees and stakeholders can report suspected fraudulent activities without fear of retaliation.
5	11	NA	Fraud Investigation Procedure Great care must be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way. The fraud investigation shall consist of gathering sufficient information about specific details and performing those procedures that are necessary to determine whether fraud has occurred, the loss or exposures associated with the fraud, who was involved in it and the fraud scheme.	Fraud Investigation Procedure Deletion

			The members of the Fraud Investigation Team shall comply with Fraud investigation procedure manual at all times. In performing their duties under this Policy, the members of the Fraud Investigation Team should have free and unrestricted access to all Company records and premises, whether owned or rented, and the authority to examine, copy and/or remove all or any portion of the contents of files, desks, cabinets and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation.	
5	11	NA	Disciplinary Measures Based on the investigation findings, staff and intermediary accountability and complicity disciplinary measures will be decided. Efforts will be made to recover the loss amount fully. Based on the nature of the fraud, an internal committee may decide on suitable penal action as per the grid (disciplinary action matrix/ service rules) defined or pursue the matter with other law enforcement agencies for appropriate action against the concerned person(s). An employee, intermediary and agent shall be subject to disciplinary action, including the termination of their employment, if the employee fails to cooperate in an investigation, or deliberately provides false information during an investigation.	Disciplinary Measures Deletion

5	11	NA	Policy Requirements Loss monitoring and recovery SHAIC shall keep a track of all losses to be recovered from the fraudsters and monitor the same periodically.	NA
5	11	3	Reporting 3.1 Internal Reporting Nodal Officer in every Zone/Area Office shall provide a list of cases of fraud occurring in their jurisdiction on monthly basis to the Nodal Officer in Corporate Office. Marketing, HR and Claims Team to report any fraud identified to the risk and investigation team as and when observed. The information received from all the offices will be collated by the Nodal Officer and this will be shared with all other Nodal Officers. Besides, this information will be passed on to the Training Dept. for dissemination in Training sessions conducted for employees including Agents. Audit and Inspection Dept. as well as Vigilance Dept. will be given this information to be used during their routine exercises. 3.2 External Reporting SHAIC shall furnish the statistics on various fraudulent cases which come to light and action taken thereon shall be filed with the Authority in forms FMR 1 and FMR 2 providing details of i. Outstanding fraud cases; and ii. Closed fraud cases Within 30 days of the close of every financial year.	Reporting SHAIC shall furnish the statistics on various fraudulent cases which come to light and action taken thereon shall be filed with the Authority in forms FMR 1 providing details of i. Outstanding fraud cases; and ii. Closed fraud cases Within 30 days of the close of every financial year. Fraud committed by distribution channels registered by IRDAI, shall be immediately reported to IRDA

5	12	NA	Appendices Annexures Annexure 1: Illustrative List of function wise frauds 1. Marketing & Communication a. Intentional misrepresentation of product features or making false claims for selling a product on social media or press media b. Intentional circulation of obsolete products brochures resulting in damage to the reputation of SHAIC c. Unauthorised usage of SHAIC name / logo to gain undue benefits d. Circulation of inflated financial analytics of SHAIC deliberately e. Intentionally posting Sensitive / Confidential information on social media or press media resulting in reputational / financial loss to the organization 2. Administration a. Employee steals assets including cash from SHAIC, either by physically taking it or diverting it in some other way leading to inventory shrinkage b. Vendor Fraud includes employee colluding with others to process false claims for benefits or payments or intentional non-disclosure of conflict of interest during empanelment of vendor. c. Employee colludes with the vendor and provides information about SHAIC's budget of procuring an asset or pricing quoted by other vendors for kickbacks from the vendor d. Employee intentionally submits inflated expense claims, false reimbursement claims, forged receipt for reimbursement or claims the expenses multiple times against same bill. e. Procurement fraud includes over-ordering of assets and selling them below their true value for personal gains f. Employee uses SHAIC's assets in an unauthorized manner for personal gains.	Appendices Deletion
---	----	----	---	---

		3. Finance a. Employee creates fictitious vendor account or manipulates the account of an existing vendor for generating false payments for personal gain b. Employee forges signature on the cheque or alters the payee details, amount or other details mentioned on the cheque or creates an unauthorized cheque for personal gain. c. Employee submits and/or approves fake/tampered food bills, vendor bills, hotel bills, travel bills, to gain monetary benefits. 4. Human Resource a. Hiring an employee without proper credential check, criminal/dubious background and employment records verification b. Payroll employee creates a fake employee in payroll records and diverts the salary in his own account Ex employee is intentionally kept active on the payroll and salary payable is diverted to another account for personal gain. c. Salary is intentionally transferred to matching or duplicate salary bank accounts of an employee for kickbacks Falsification of entries in attendance record resulting in inflated salary processing d. Marking attendance in the system for self- whilst the employee is absent from duty or marking attendance in the system for another employee, whether the other employee is on duty or absent from duty e. Allowing another person to mark attendance on behalf of an employee, whether the employee allowing is on duty or absent from duty f. Dual employment g. Hiring relatives leading to conflicts of interest or otherwise not in accordance with HR Policy of SHAIC (including contractual employees)	
--	--	---	--

		h. On-boarding a vendor without proper background check and documents verification 5. Information Technology a. Employee intentionally shares confidential information pertaining to SHAIC or its customers or its employees to the third party. b. Employee steals or intentionally shares client list, account numbers, personal information with another person. c. Not disabling email/system access of inactive employees resulting in unauthorized usage by others d. Employees fraudulently breaking IT rules built to safeguard the data systems 6. Legal & Compliance a. Seek kickbacks / favours for not initiating Governance Action or for lower severity punishment b. Suppress evidences to avoid Governance action 7. Operations a. Overriding actual decision in family / friend's policies at issue at standard rate (otherwise would have been over-rated or declined/postponed) b. Approving fraudulent claims by suppressing actual reports for monetary gain c. Cancelling & refunding policy premium post FLC period without following due approval process resulting in substantial premium loss d. Misappropriation of office cash or misuse of cheques or any other payment instrument e. Tampering office documents to conceal any operational fraud done by an employee f. Manipulation of bank account details for misappropriation of funds g. Misuse of credit cards, debit cards or net banking or any other online payment methods for misappropriation of funds h. Any other fraud within the operation function 8. Sales Function	
--	--	--	--

			a. Misappropriation of customer money Anti-Fraud Policy Page 16 of 19 b. Forging signatures in documents c. Misrepresentation of critical details of customers KYC documents of customers misused or tampered d. Recruiting relatives as direct reportee under them without disclosing relationships e. Impersonating like customer in Verification calls or any other call done by SHAIC to the Customer f. Giving false Agents' Confidential Reports or Moral Hazard Report hiding the financial or health status of the life assured, including physical existence of the life assured g. Tampering any document including Proposal form, Benefits illustration, payment instruments, Age proof, KYC documents with the intention of defrauding SHAIC h. Colluding with the Medical Centre and arranging for medical examination reports without the life assured not undergoing medical examination i. False certification of copies of documents j. Fraudulent or unauthorised usage of SHAIC's letterhead & logo k. Delay in deposit of premium remitted by the Policyholder, to SHAIC	
5	12	4.2	Appendices List of applicable regulations NA	Appendices List of applicable regulations - Date of issuance - 09-10-2025 - Ref. No - IRDAI/IID/GDL/MISC/112/10/2025 - Name of Legislation - Insurance Regulatory and Development Authority of India (Insurance Fraud Monitoring Framework) Guidelines, 2025