IndiaFirst Life Insurance Company Limited

Anti-Fraud Policy

Index

1. Introduction

Fraud is a broad legal concept. Unlike error, fraud is intentional and usually involves deliberate concealment of the facts. It may involve directors, management, employees or third parties and may involve one individual or collusion.

Today's business environment is likely to increase vulnerability to fraud risk, due to technological advances, growing complexity of organizations, increasingly transient employees, amongst others. Fraud is a significant business risk that needs to be managed like all other business risks. Fraud can have a devastating effect on organisations as it could result in a significant financial loss and have other long-term business repercussions such as loss of public trust. The risk of fraud can be reduced through a combination of prevention, deterrence and detection measures.

Since fraud may be difficult to detect because it often involves concealment through falsification of documents and collusion among staff or third parties, it is important to place a strong emphasis on fraud prevention, which reduces opportunities for fraud to take place, and fraud deterrence, which persuades individuals that they should not commit fraud because of the likelihood of detection and punishment.

One of the values promoted at IndiaFirst Life Insurance Company Limited (hereinafter referred to as the "**Company**") is 'Be Honest'. We at IndiaFirst Life focus on our principles and are committed to maintaining the highest standards of ethics and do not tolerate any form of fraud or dishonesty. All individuals regardless of position, title, or tenure are expected to remain vigilant and are responsible for preventing, detecting fraud and also report any suspicious fraudulent activity.

2. Objectives

The "Anti-Fraud Policy" has been framed to provide a system for prevention and detection of fraud, reporting of any fraud that is detected or suspected and fair dealing of matters pertaining to fraud.

The objective of this policy is to establish a consistent and responsible attitude to fraud and dishonesty within the company with the aim of:

- Minimising the potential and actual incidence of fraud
- Detecting incidents of fraud
- Minimising the risk of subsequent losses
- Improving the chance and scale of recoveries
- Reducing adverse commercial effects
- Making a clear statement to vendors, customers and others that the company will not tolerate fraud
- Enhancing the climate of honesty which the company seeks to maintain
- Reducing the opportunities for fraud in co-operation with other organisations

3. Scope

This policy identifies the measures that the Company shall implement to prevent, deter and detect fraud in the context of three fundamental elements:

- Create and maintain a culture of honesty and high ethics, including via the understanding and awareness of risks and controls;
- Identify and assess the risks of fraud and implement the processes, procedures and controls needed to mitigate the risks and reduce the opportunities for fraud; and
- Develop an appropriate oversight process.

Specifically, this policy aims at:

- Ensuring that management is aware of its responsibilities for the prevention and detection of fraud and for establishing procedures to prevent fraud and/or detect fraud on its occurrence;
- Providing a clear guidance to employees and others dealing with the Company, forbidding them from involvement in any fraudulent activity and the action to be taken by them when they suspect any fraudulent activity;
- Providing a mechanism for employees and officers of the Company to report any incident of fraud or alleged incident of fraud and protect the employees and officers of the Company who make a disclosure against their managers and/or fellow employees in certain defined circumstances from harassment and/or dismissal;
- Providing a clear guidance on how investigations into fraudulent activities will be conducted;
- Providing assurance that any and all suspected fraudulent activities will be fully investigated and dealt with;
- Providing assurance to one and all that any and all suspected fraudulent activities will not be allowed or tolerated; and
- Ensuring preventive measures and internal control procedure enhancement, subsequent to any fraud being identified, are strengthened in a speedy manner.

This policy applies to all employees and officers of the Company including contractual staff and directors in the employment of the Company, as well as shareholders, agents and other insurance intermediaries, service providers, consultants, vendors, contractors and subcontractors, prospective and existing customers and/or other parties with a business relationship with the Company. Any required investigative activity will be conducted without regard to the suspected wrongdoer's length of service, position/title or relationship to the Company.

4. Classification of Insurance Frauds:

Fraud 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 the company's status;
- Abusing responsibility, a position of trust or a fiduciary relationship.

In order to adequately protect itself from the financial and reputational risks posed by insurance frauds, the policy is designed to prevent, detect, monitor and mitigate occurrence of frauds in the company. The policy includes measures to protect the Company from the threats posted by the following broad categories of frauds:

a) **Policyholder Fraud and/or Claims Fraud** - Fraud against the company in the purchase and/or execution of an insurance product, including fraud at the time of making a claim.
b) **Intermediary Fraud** - Fraud perpetuated by an insurance agent/Corporate Agent/intermediary/Third Party Administrators (TPAs) and vendors against the company and/or policyholders.
c) **Internal Fraud** - Fraud/ misappropriation against the company by its Director, Manager and/or any other officer or staff member (by whatever name called).
d) **Third party Fraud –** Fraud committed by third parties against the insurer and the general public which primarily includes activities such as fake/forged receipts and/or policy document
e) **Online Fraud** – This type of fraud is typically a third party fraud, however, this could involve any of the following types of frauds –

- **Buyer side frauds**: Where buyers file fraudulent claims or compromised payment cards
- **Merchant side frauds**: Frauds committed by any of the merchant partners of the Company which would include non-remittance of premium collected on behalf of the Company and/or incorrect charge backs etc
- **Cyber security frauds**: Transactions effected through fake or stolen credit card/bank accounts to carry out a transaction in the web portal of the Company. Threat of confidential data of the Company being comprised due to any cyberattack/hacking of the Company systems
- **Other Frauds**: Any other type of fraud which does not fall in any of the above categories.

While fraudulent activity could have a very wide range of coverage, the following are some of the act(s) which constitute fraud. The list is only illustrative and not exhaustive:

- Forgery or alteration of an application form or any document submitted by the customer.
- Forgery or alteration of any document or account belonging to the Company.
- Forgery or alteration of cheque, bank draft or any other financial instrument etc.
- Misappropriation of funds, securities, supplies or others assets by fraudulent means etc.
- Falsifying records such as payroll, removing the documents from files and /or replacing it by a fraudulent note etc.
- Making fraudulent or false noting
- Willful suppression of facts/deception in matters of appointment, placements, submission of reports, etc. as a result of which a wrongful gain(s) is made to one and wrongful loss(s) is caused to the others.
- Utilizing Company funds for personal purposes.
- Authorizing or receiving payments for goods not supplied or services not rendered.
- Destruction, disposition, removal of records or any other assets of the Company with an ulterior motive to manipulate and misrepresent the facts so as to create suspicion/suppression/cheating as a result of which objective assessment/decision would not be arrived at.
- Electronic fraud or ethical hacking

- Any other act that falls under the gamut of fraudulent activity.

A list of indicators and types of fraud are enclosed as per Appendix 1, Annexure I and Annexure-II respectively.

5. Fraud Risk Governance - Creating a Culture of Honesty and High Ethics

The Board of Directors, managers and officers set the "tone at the top" for ethical behaviour by behaving ethically and openly communicating expectations for ethical behaviour to employees.
The Anti-Fraud policy is clearly communicated to all officers and staff members of the Company in an understandable fashion. The policy shall be communicated by the Head Governance and Company Secretary to all the Employees of the Company and other persons dealing with the Company, through email, circular, or display on the Notice Board/ display on the Intranet. In addition, 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 the Company, in order to clearly communicate expectations for ethical behavior to staff members.

Directors, employees and contractors shall internally self-disclose potential or actual conflicts of interest to Head Governance and Company Secretary.

As part of the Company's due diligence for fraud detection and mitigation, background checks on new employees and personnel (management and staff) / insurance agent / corporate agent / intermediary(including the educational background, work experience, criminal records, etc.) shall be carried out in order to prevent fraud at the source. Background checks shall be duly formalized and documented in writing. Exit interviews shall be conducted with terminated, resigning or retiring employees regardless of their position to identify potential fraud and vulnerabilities to fraud that may be taking place in the Company. Furthermore, staff rotation and tying employee evaluations to compliance reviews and internal control reviews can also help to prevent fraud at the source.

6. Fraud Risk Assessment - Evaluating the Risks of Fraud and Implementing Anti-fraud processes and controls

The Company shall be proactive in reducing fraud opportunities by (1) identifying and measuring fraud risks, (2) taking steps to mitigate identified risks (including IT and cyber risks), (3) implementing and monitoring appropriate preventive and detective internal controls and other deterrent measures and (4) coordinating with law enforcement agencies.

Management has the primary responsibility for establishing and monitoring all aspects of the Company's fraud risk assessment and prevention activities and performing the fraud risk assessment.

Individuals from throughout the organization with different knowledge, skills and perspectives (e.g. accounting/finance, non-financial business units and operations personnel, legal & compliance, risk management, internal audit, etc.) shall be involved in the fraud risk assessment.

Through the fraud risk assessment, the vulnerability of the Company to fraudulent activities (for example, misappropriation of assets, corruption, fraudulent financial reporting, etc.) is considered, as well as whether any of those exposures could result in a material misstatement

of the financial statements or material loss to the Company. The fraud risk assessment shall identify where fraud may occur and who the perpetrators might be.

The nature and extent of the fraud risk assessment shall be commensurate with the size of the Company and the complexity of its operations. It shall be performed, documented and updated periodically to identify potential fraud schemes, scenarios and events that need to be mitigated. Updates shall include considerations of changes in operations, new information systems, changes in job roles and responsibilities, internal audit findings, new or evolving industry trends, amongst others.

The fraud risk assessment shall be performed at all appropriate levels within the organization and shall be coordinated with the operational risk assessment. The fraud risk assessment shall include fraud risk identification, fraud risk likelihood and significance and fraud risk response.

Although management has the primary responsibility for performing the fraud risk assessment, it is also critical that employees outside of management are involved in the fraud risk assessment. It is important that the business process owners or those who have significant knowledge, control or influence over the activities within a significant business process or cycle are involved in the fraud risk assessment exercise.

Once the fraud risk assessment has taken place, management shall reduce and eliminate identified fraud risks by making changes to the Company's activities and processes and identify the processes, controls and other procedures that are needed to mitigate the identified fraud risks. Effective and appropriate internal controls, whether automated or manual, which include a well-developed control environment, an effective and secure information system and appropriate control and monitoring activities, are essential to reduce and eliminate identified fraud risks.

Internal Audit shall play an active role in the development, monitoring and ongoing assessment of the fraud risk management program of the Company. Specifically, Internal Audit shall independently evaluate whether internal controls designed to reduce the risk of fraud are adequate and effective. Internal Audit shall assist management throughout the fraud risk assessment exercise, review the result of the assessment, independently assess the ability of existing controls to prevent the occurrence of fraud, propose corrective measures and present the outcome of the fraud risk assessment as part of the internal audit report for review and comments.

7. Roles & Responsibilities - Developing an Appropriate Oversight Process

Management is responsible for designing and implementing systems, procedures and internal controls for the prevention and detection of fraud commensurate with the nature and size of the organization and along with the Board of Directors, for ensuring a culture and environment that promotes honesty and ethical behaviour.

The Managing Director and Chief Executive Officer of the Company initiates and support anti-fraud measures.

Each member of the management team shall be familiar with the types of improprieties that might occur within his or her area of responsibility and be alert for any indication of irregularity. Through the Audit Committee, the Board of Directors shall evaluate management identification of fraud risks, implementation of antifraud measures and creation of the appropriate "tone at the top".

The Vigilance and Ethics Committee that reports to the Audit Committee of the Board shall also ensure that the management implements appropriate fraud deterrence and prevention measures. The Vigilance and Ethics Committee shall receive periodic reports describing the nature, status and disposition of any fraud or unethical conduct.

The Vigilance and Ethics Committee shall establish an open line of communication with members of management one or two levels below senior management to assist in identifying fraud at the highest levels of the organization or investigating any fraudulent activity that might occur. Vigilance and Ethics Committee will place on a half yearly basis, the summary of the critical issues and material findings to the Audit Committee for noting.

Employees and officers at every level, in every department and at every location 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 current procedures in place.

Internal Audit shall assist in the deterrence of fraud by examining and evaluating the adequacy and the effectiveness of the system of internal controls and by conducting proactive auditing to search for fraud. In addition, by carrying out fraud audits, Internal Audit shall proactively detect indications of fraud in those processes or transactions where analysis indicates the risk of fraud to be significant or high, gather information and make appropriate recommendations.

Risk Management shall assist management in identifying and assessing fraud risks and help management to design specific controls to mitigate fraud risks.

Risk Management and Audit shall assist management in drafting anti-fraud policies and procedures and conducting fraud awareness training, thus helping in educating employees about fraud prevention and detection.

8. Fraud investigation, fact finding and corrective action

This policy applies to all activities undertaken by or on behalf of the company. It applies to internal fraud i.e. fraud against an employee and external fraud i.e. fraud against an external party viz. employees of a partner or vendor or against the customer/policyholder.

Any employee who suspects dishonest or fraudulent activity shall notify the Internal Audit & Fraud Control Unit immediately, and should not attempt to personally conduct investigations or interviews/ interrogations related to any suspected fraudulent act. Any alleged or suspected incident of fraud shall be reported in writing so as to ensure a clear understanding of the issues raised.

The frauds are required to be reported to

K R Viswanarayan
Head Governance and Company Secretary
IndiaFirst Life Insurance Company Limited

Reports should be made 'in confidence'. The person to whom the fraud or suspected fraud has been reported must maintain the confidentiality with respect to the reporter. Such matter should under no circumstances be discussed with any other person who is not supposed to know about/ or is not an authorized person in such matters.

Anonymous disclosures or disclosures containing general, non-detailed or offensive information will be reviewed and investigated in detail. Based on the severity and materiality of the fact, the Head Governance and Company Secretary will assess the case its entirety and will exercise his judgement on cases to be reported to the Vigilance and Ethics Committee. A record of all anonymous disclosures, investigation findings and the actions taken should be maintained by the Internal Audit & Fraud Control Unit

The following actions shall be taken in response to an alleged or suspected incident of fraud:

- A thorough investigation of the incident shall be conducted.
- Appropriate and consistent actions shall be taken against violators.
- Relevant controls shall be assessed and improved.
- Communication and training shall occur to reinforce the Company's values, code of conduct and expectations.

All employees shall cooperate fully with an investigation into any alleged or suspected fraud. Details of the investigation process are as follows:

***Logging*:** The Internal Audit & Fraud Control Unit maintains a centralized internal fraud database where all internal fraud data losses and recoveries are logged. Upon discovery or reporting of an internal fraud case, the Fraud Control Unit Head opens a case file, logs the case in the centralized internal fraud database and assigns a case number to the case. This enables the Company to track the resolution progress.

***Preliminary Analysis*:** Then, the alleged internal fraud case is reviewed jointly by the Head of Governance, the Head of Human Resources and the Head of Internal Audit to determine:

- Whether the case should be investigated;
- Who should investigate the case;
- The types of resources needed to conduct the investigation;
- Who will be interviewed during the course of the investigation and how information will be gathered;
- The timeframe for completion; and
- How results will be reported and to whom.

The Head of Governance, the Head of Human Resources and/or the Head of Internal Audit shall be excluded from the preliminary analysis or the subsequent investigations if the alleged or suspected internal fraud case involves him/her.

***Fraud Investigation Team*:** During the preliminary analysis, the types of resources needed to conduct the investigation are duly determined (e.g. internal audit, human resources, legal

and compliance, risk management, external legal counsel, forensic auditors, technical experts, etc.). The Internal Audit & Fraud Control Unit has the primary responsibility for the investigation of all suspected or alleged internal fraudulent acts as defined in this document.

As a minimum, the investigation shall be done by team of Internal Auditors, Human Resources and Legal & Compliance staff members.

Technical resources may be drawn upon as necessary to augment the investigation (e.g. Information Technology, Claims, Underwriting etc) provided that they are independent from the case and unbiased.

***Investigations*:** 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 (how it happened).

The members of the Fraud Investigation Team will 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.

The alleged fraudster will be informed of the allegations as soon as reasonably practicable. This may not be until the initial stages of the investigation have taken place.

The investigations shall take place on legal restrictions to ensure that findings are admissible in court. Investigatory or disciplinary hearings and evidence gathering will always be carried out with the assistance and under the supervision of legal counsel (either internal and/or external). The Internal Audit & Fraud Control Unit shall timely take in their custody all relevant records, documents and other evidence to protect them from being tampered with, destroyed or removed by the suspected perpetrators of fraud or by any other party under his/her influence. The full records of the investigation, including interview notes, shall be kept secure. The investigations shall be kept as confidential and private as possible to ensure the least amount of disruption to the Company and maintain the process integrity at all times. Confidential information will be shared only on a “need-to-know” basis.

The investigations shall be completed normally within **forty-five (45) days** from the disclosure or discovery of the fraud case. However, the Vigilance and Ethics Committee has the discretion to extend the duration of the investigation, depending upon the complexity of the case

The conclusion and results of the investigations must be duly documented in writing. The fraud report regarding the results of the investigations and the corrective actions shall capture at least the fraud incident description, the fraud perpetrator details, the estimated fraud loss and recovery amounts, the controls implications and the resolution. Management is responsible for resolving fraud incidents. The fraud report along with the recommendation is shared with the Vigilance and Ethics Committee for decision.

Once investigations are completed and risk findings are identified, thereafter the Legal team shall initiate and take necessary action by approaching Law Enforcement Agencies, whenever appropriate.

***Decision*:** Once the investigation is completed and if it substantiates that fraudulent activities have occurred, the Internal Audit & Fraud Control Unit shall recommend to the Chief Executive Officer of the Company to take such disciplinary or corrective actions (e.g. employee discipline, any referral to the applicable law enforcement agency, changes to processes or internal controls, etc.), as they may deem fit.

If employees are involved in fraudulent activity, an appropriate action will be taken by the Internal Audit & Fraud Control Unit in consultation with the Human Resources team.

Appropriate action may include any of the following:

- Internal disciplinary action such as Issuing Warning letter to the fraudulent employee
- Reduce/ slash the incentive payments due to the employee
- Termination, suspension with or without pay, demotion or warnings
- Termination of contracts with the fraudulent vendors.
- Civil lawsuits
- Register First Information Report (FIR)/police complaint against fraudulent individual
- Recover loss caused by fraudulent activity from fraudulent employee/vendor
- Initiate legal proceedings against the fraudulent individual/group of individuals

All actions taken in response to an established act of fraud must be approved by the Vigilance and Ethics Committee.

Any decisions to prosecute by way of civil proceedings or refer the examination results to the appropriate law enforcement and/or regulatory agencies for independent investigation will be taken in conjunction with legal counsel by the Chief Executive Officer of the Company or by the Board of Directors of the Company (whenever they exceed the authority limits granted to him/her by the Board), as will final decisions on disposition of the case.

All internal investigations must be completed within 60 days from date of disclosure of the case. However, the Vigilance and Ethics Committee can extend the duration of the investigation depending upon the complexity of the case. The legal notices must be issued within 45 days from date of completion of the investigation and FIR with the police must be filed within 60 days of completion of the fraud investigation.

Where warning letter has been issued to the fraudulent individual/group of individual, any second incident will be treated gravely and all investigation reports shall mention the first incident so occurred.

The Vigilance and Ethics Committee will be timely informed of such decisions. The Internal Audit & Fraud Control Unit will monitor the implementation of the resolution to ensure that proper corrective action was taken and report to the Audit Committee accordingly. Only after the resolution has been verified, the case can be closed.

***Reporting*:** The Head - Internal Audit & Fraud Control Unit will keep track of all cases and timely and periodically submit a report to Vigilance and Ethics Committee about the status and results of the investigations and corrective actions taken, along with the report of the investigators.

9. **Reporting of Frauds**

Any one (full time and part time employees or persons appointed on adhoc/ temporary/ contract basis, trainees, apprentices, representatives of vendors/ suppliers/ contractors /consultants /service providers or any other agency doing any business with IndiaFirst) as soon as he / she comes to know of any fraud or suspects a fraud or notices any other fraudulent activity, he/she must report such incident(s) immediately without delay to the Internal Audit & Fraud Control Unit

The reporting of the fraud should be in writing. In case the reporter is not willing to furnish a written statement of fraud but is in a position to give sequential and specific transaction of fraud/suspected fraud, then Internal Audit & Fraud Control Unit on receiving the information should record such details in writing as narrated by the reporter and also maintain the details of the identity of the official / employee / other person reporting such incident.

In case, the management finds the fraud/ suspected fraud reported is motivated or vexatious, it shall be at liberty to take appropriate steps against the person reporting the fraud.

10. Due Diligence:

Every employee (full time, part time, temporary, contractual), representative of vendors, consultants, service providers or any other agency(ies) doing any type of business with the company, is expected and shall be responsible to ensure that there is no fraudulent act being committed in their areas of responsibility/control. As soon as it is learnt that a fraud or suspected fraud has taken or is likely to take place they should immediately appraise the same to the concerned official as per the procedure.

All officers shall share the responsibility of prevention and detection of fraud and for implementing the Anti-Fraud Policy. It is the responsibility of all officers to ensure that mechanisms are in place within their area of function to:-

- Inform every one working with/ under him/her about ‘Anti- Fraud Policy’,
- Familiarize each employee with the types of improprieties that might occur in their area.
- Educate employees about fraud prevention and detection.
- Create a culture whereby employees are encouraged to report any fraud or suspected fraud which comes to their knowledge, without any fear of victimization.
- Promote employee awareness of ethical principles and values of the Company

A disclosure about the 'Anti-Fraud Policy' will be made a part of the RFP process, so as to make every one aware of and not to indulge or allow anybody else working in their organization to indulge in fraudulent activities while dealing with the company

The following disclaimer may be made a part of the RFPs issued by the Company:

Fraud Prevention Policy of IndiaFirst:

- Everyone may take a note that an "Anti-Fraud Policy" is being followed at IndiaFirst Life Insurance, which provides a system for prevention/ detection/ reporting of any fraud. It also forbids everyone from involvement in any fraudulent activity and that where any fraudulent activity is suspected by any one, the matter must be reported to Fraud Control Unit, as soon as he /she comes to know of any fraud or suspected fraud or notice any other fraudulent activity.

- Anonymous complaints received, if not supported by the relevant evidence or not easily verifiable by the Company, may not be acted upon.
- All reports of fraud or suspected fraud shall be handled and shall be coordinated by the Fraud Control Unit.
- A copy of the 'Anti-Fraud Policy' is available on the official web-site of the company

11. **Vigilance and Ethics Committee**

The Vigilance and Ethics Committee shall be responsible for the following:

- Laying down procedures for internal reporting from/and to various departments.
- Creating awareness among employees/ intermediaries/ policyholders to counter insurance frauds.
- Furnishing various reports on frauds to the Authority as stipulated in this regard.
- Furnish periodic reports to the Board of the Directors of the Company.

12. Fraud incident reporting

The Fraud Incident Reporting shall capture crucial information regarding each fraud incident, including description, fraud perpetrator details, loss and recovery estimates, control implications and proposed or completed actions taken. The Chief Financial Officer shall be provided with a summary of internal fraud cases (either alleged, credible or proven) that may jeopardize financial reporting.

At the meeting, the Vigilance and Ethics Committee shall be provided with a condensed report for review of reported fraud cases [either internal (all cases) or external (above a defined threshold)], trends, early results from investigations underway and remediation taken by management to address any identified control weakness.

Any public communications and comments by management to the press, law enforcement or other external parties in relation to incidents of fraud shall only be made by authorized spokespersons and coordinated through legal counsel and corporate communications.

13. **Reports to the Authority:**

The statistics on various fraudulent cases investigated/highlighted and action taken thereon shall be filed with Insurance Regulatory and Development Authority ("IRDA") IRDA in forms FMR 1 and FMR 2 (as prescribed by IRDA vide its Circular bearing ref. no. IRDA/SDD/MISC/CIR/009/01/2013, dated January 21, 2013) providing details of

(i) outstanding fraud cases; and

(ii) closed fraud cases every year

within 30 days of the close of the financial year , i.e. on or before the 30th of April

As part of the responsibility statement which forms part of the management report filed with the Authority under the *IRDA (Preparation of Financial Statements and Auditors Report of Insurance Companies) Regulations, 2002*, the management is also required to disclose the

adequacy of systems in place to safeguard the assets for preventing and detecting fraud and other irregularities, on an annual basis.

14. Preventive mechanism:

The company will inform both potential stakeholders and existing stakeholders about the policy. The company shall appropriately include necessary caution in the relevant documents, duly highlighting the consequences of submitting false statement and/or incomplete statement, for the benefit of the policyholders, claimants and the beneficiaries.

15. **Administration and Review of this Document**

The Head Governance and Company Secretary is responsible for the administration, revision, interpretation and application of this document, as well as of the related Internal Fraud Policy Statement. These documents will be reviewed and revised at least annually in line with IRDA guidelines. Any revised version shall be submitted to the Audit Committee of the Board of Directors for review and the Board of Directors of the Company for final approval.

Appendix I

Illustrative List of Insurance Frauds

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

1. Internal Fraud:

- Embezzlement (i.e. misappropriation of money, securities, supplies, property or other assets);
- Fraudulent financial reporting (e.g. forging or alteration of accounting documents or records;
- Cheque fraud (i.e. forgery or alteration of cheques, bank drafts or any other financial instrument);
- Overriding decline decisions so as to open accounts for family and friends
- inflating expenses claims/over billing
- paying false (or inflated) invoices, either self-prepared or obtained through collusion with suppliers
- permitting special prices or privileges to customers, or granting business to favored suppliers, for kickbacks/favors
- Forgery or alteration of documents or accounts belonging to the Company
- Embezzlement (i.e. misappropriation of money, securities, supplies, property or other assets)
- falsifying documents
- Selling insurer's assets at below their true value in return for payment.
- Conflicts of Interest resulting in actual or exposure to financial loss;
- Payroll fraud;
- Tax evasion;
- Unauthorized or illegal use of confidential information (e.g. profiteering as a result of insider knowledge of company activities);
- Unauthorized or illegal manipulation of information technology networks or operating systems;
- statements; intentional failure to record or disclose significant information accurately or completely);
- Improper pricing activity;

2. Policyholder Fraud and Claims Fraud:

- Exaggerating damages/loss
- Staging the occurrence of incidents
- Reporting and claiming of fictitious damage/loss
- Medical claims fraud
- Fraudulent Death Claims
- Spurious calls to policyholders promising rewards or bonuses on surrender of insurance policies
- Spurious calls to policyholders promising bonus declared by IRDA
- Intimation received by policyholders of the following :

- Unauthorized transactions being initiated on their policies such as switches, withdrawals, surrenders etc
- Unauthorized changes in contact details
- Cash, cheques handed over by policyholders to agents however, they have not received any intimation from the company of its receipt

3. Intermediary fraud:

- Premium diversion-intermediary takes the premium from the purchaser and does not pass it to the insurer
- Inflates the premium, passing on the correct amount to the insurer and keeping the difference
- Non-disclosure or misrepresentation of the risk to reduce premiums
- Commission fraud insuring non-existent policyholders while paying a first premium to the insurer, collecting commission and annulling the insurance by ceasing further premium payments.

4. Third party Fraud:

- Fake or forged receipts and/or policy documents issued by third parties
- Spurious calls by third parties to customers promising them inflated returns for purchasing new policies or on surrender of their existing policies

5. Online Fraud

- Buyers filings fraudulent claims or making premium payments using compromised payment cards
- Merchant side frauds: Frauds committed by any of the merchant partners of the Company which would include non-remittance of premium collected on behalf of the Company and/or incorrect charge backs etc
- Cyber security frauds: Transactions effected through fake or stolen credit card/bank accounts to carry out a transaction in the web portal of the Company.
- Data leakage : Threat of confidential data of the Company being comprised due to any cyber attack/hacking of the Company systems
- Other Frauds: Phishing emails sent to customers promising them inflated returns. Using social engineering techniques to wrongly influence the customers to share their identity details

Annexure II

Indicators of Fraud

- Missing expenditure vouchers and unavailable official records
- Crisis management coupled with a pressured business climate
- Profitability declining
- Excessive variations to budgets or contracts
- Refusals to produce files, minutes or other records
- Related party transactions
- Increased employee absences
- Borrowing from fellow employees
- An easily led personality
- Covering up inefficiencies
- No supervision
- Staff turnover is excessive
- Figures, trends or results which do not accord with expectations
- Bank reconciliations are not maintained or can't be balanced
- Excessive movement of cash funds
- Multiple cash collection points
- Remote locations of any event.
- Unauthorized changes to systems or work practices
- Employees with outside business interests or other jobs
- Large outstanding bad or doubtful debts
- Officers with excessively flamboyant characteristics
- Employees suffering financial hardships
- Placing undated/post-dated personal cheque in petty cash
- Employees apparently living beyond their means
- Heavy gambling debts
- Signs of drinking or drug abuse problems
- Conflicts of Interest
- Lowest tenders or quotes passed over with scant explanations recorded
- Employees with an apparently excessive work situation for their position
- Managers bypassing subordinates
- Subordinates bypassing managers
- Excessive generosity
- Large sums of unclaimed money
- Large sums held in petty cash
- Lack of clear financial delegations
- Secretiveness
- Apparent personal problems
- Marked character changes
- Poor morale of employees
- Excessive control of all records by one officer
- Poor security checking processes over staff being hired
- Unusual working hours on a regular basis
- Refusal to comply with normal rules and practices
- Personal creditors appearing at the workplace
- Not availing of leave
- Excessive overtime
- Large backlogs in high risk areas

- Lost assets
- Absence of controls and audit trails.
- Socializing with clients – meals, drinks, holidays
- Seeking work for clients
- Favorable treatment of clients – e.g. passing sensitive information to selected bidders.
- Altering contract specifications
- Contract not completed to specification
- Contractor paid for work not done.
- Grants not used for specified purpose –eg Leasing capital equipment instead of purchasing them

Annexure III

Common Methods and Types of Fraud

- Payment for work not performed
- Forged endorsements
- Altering amounts and details on documents
- Collusive bidding
- Overcharging
- Writing off recoverable assets or debts
- Unauthorized transactions
- Selling information
- Altering sales records
- Cheque made out to false persons
- False persons on payroll
- Unrecorded transactions
- Transactions (expenditure/receipts/deposits) recorded for incorrect sums
- Cash stolen
- Supplies not recorded at all
- False official identification used
- Damaging/destroying documentation
- Using copies of records and receipts
- Using imaging and desktop publishing technology to produce apparent original invoices
- Charging incorrect amounts with amounts stolen
- Transferring amounts between accounts frequently
- Delayed terminations from payroll
- Bribes
- Over claiming expenses
- Skimming odd pence and rounding
- Running a private business with official assets
- Using facsimile signatures
- False compensation and insurance claims
- Selling waste and scrap.